AU/ACSC/7712/AY09

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

USAF Cyber Capability Development:

A Vision for Future Cyber Warfare

&

A Concept for Education of Cyberspace Leaders

By

Paul D. Williams, Major, USAF, Ph.D.

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisors:
Col (ret) Roger Philipsek, USAF
Lt Col Michael Linschoten, USAF

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **APR 2009**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE
USAF Cyber Capability Development: A Vision for Future Cyber Warfare & A Concept for Education of Cyberspace Leaders

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Command And Staff College Air University Maxwell Air Force Base, Alabama

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

significant and interrelated problems are hindering the Air Force¡®s development of cyber warfare capabilities. The first is a lack of awareness about why the AF has chosen to take cyber warfare on as a core capability on par with air and space. The second stems from the lack of a commonly understood vision for how future AF cyber warfighting capabilities will support our national security objectives. This research project addressed these problems by exploring the following questions: - What types and ranges of offensive and defensive cyber effects might the Air Force provide, both externally for the combatant commanders and internally for self-defense, in the near and medium term futures? - How should the Air Force develop and make those capabilities available to combatant commanders and internally? - How might the Air Force nurture the cyber-oriented leaders who will envision and build the cyber capabilities needed in the future? The contributions of this research include a strategic vision for future cyber warfare capabilities that support both the combatant commanders and internal service needs. It also introduces a means of developing cyber warrior-scholars who will shape the cyber warfare domain of the future. The vision for future capabilities is expressed through a set of vignette/discussion pairs. In ¨Da Day in the Life¡¬ prose form, each vignette describes a situation and how the forces involved in the scenario handle the situation. An analysis of the people, processes and technology of each vignette evaluates how the services may organize, train, and equip to produce the required capabilities. The cyber warrior-scholar concept is amplified by discussing how we develop advanced strategists and airpower advocates, including description of an existing Air Force graduate education program that largely meets the defined need, explores potential downsides, describes how this proposal fits into the ongoing cyber warfare force development effort, and finishes with courses of action and a recommendation. Strategy can be thought of as defining a vision of the future, and mapping out how to get there. The overall goal of this research is to spur thought about what the vision for AF cyber warfare capabilities should look like, and drive discussion about how to make that vision a reality.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**103**	

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

List of Illustrations

Page

List of Tables

List of Acronyms

Acronym	Definition	Page first defined
ACSC	Air Command and Staff College	24
ACTS	Air Corps Tactical School	7
AF	Air Force	1
AFIT	Air Force Institute of Technology	25
AFSC	Air Force Specialty Code	28
ARM	Anti-radiation munitions	60
ATC	Air traffic control	11
ATCALS	Airfield Traffic Control and Landing Systems	11
C^2	Command and Control	6
C^3	Command, Control, and communication	21
C&I	Communication and information	7
CCDR	Combatant commanders	12
CCIR	Commander's critical intelligence requirements	60
CCR	AFIT Center for Cyberspace Research	77
CNA	Computer network attack	9
CND	Computer network defense	9
CNO	Computer network operations	8
COA	Course of action	29
COG	Center of gravity	53
CTO	Cyber tasking order	55
CW	Cyber Warfare	4
DDOS	Distributed denial of service	22

Acronym	Definition	Page first defined
DOD	Department of Defense	1
EW	Electronic Warfare	5
JFC	Joint Force Commander	4
I&W	Indications and warning	22
IADS	Integrated air defense system	11
ICW	IDE Cyber Warfare	27
IDE	Intermediate developmental education	24
IFO	Influence operations	10
INOSC	Integrated network operations and security center	45
IO	Information Operations	4
IP	Internet Protocol	5
IPB	Intelligence preparation of the battlespace	19
IT	Information Technology	5
LMR	Land mobile radio	11
MILDEC	Military Deception	9
NetOps	Network creation and sustainment, or Network Operations	9
NIPRNet	Non-secure IP router network	11
NOSC	Network operations and security center	46
OPSEC	Operations security	9
OT&E	Organize, train, and equip	2
PCS	Permanent change of station	28
PLA	Chinese Peoples Liberation Army	31
PME	Professional military education	25
PSYOPS	Psychological operations	9
RF	Radio frequency	59
SAAS	School for Advanced Airpower Studies	26
SAASS	School for Advanced Air and Space Studies	24
SATCOM	Satellite Communications Networks	11
SCADA	Supervisory Control and Data Acquisition/Control Systems	11
SIGINT	Signals intelligence	31
SIMTEX	Simulator Based Training and Exercise Program	40
SIPRNet	Secure IP router network	11
SOF	Special operations force	59
TADIL	Tactical data information links	11
TTP	Tactics, techniques, and procedures	7
UAS	Unmanned aerial system	6
VIPER	Virtualized intranet platform for exercise realism	41
VOIP	Voice over IP	11
WMD	Weapons of mass destruction	21

Preface

The Air Force is working to operationalize its capability to wage warfare in cyberspace—a new and difficult challenge. In this research project, I explore three facets of the challenge: motivation for change to support cyber warfare, popular awareness of what AF cyber warfare may entail, and the development of future cyber warfare leaders through appropriately focused education.

The motivational material in Chapter 2 discusses the imperatives behind the shift from a communications-oriented force to a cyber warfare-oriented force. It attempts to address some of the common questions people have about why the AF is embarking on this path.

In Chapter 3 and Appendix A, I postulate that a lack of awareness of how to fight in cyberspace hinders the AF's progress in organizing, training, and equipping cyber warfare forces. To counter this lack of awareness I present a series of "Day in the life" vignettes which portray cyberspace operations. These vignettes are coupled with discussion about how the AF might organize, train, and equip a force to best achieve the capabilities described. The intent of this section is to describe what the goal that the AF needs to achieve in a few years should be. While the vignettes are fictional, I based their foundation upon technology we already have or will likely have in a few years: they may be fiction, but they are not science fiction.

In the essay in Chapter 4 and extended in Appendix B, I introduce a concept for how and why the Air Force should develop cyber-oriented warrior-scholars capable of shaping the Air Force fight in cyberspace. This concept is substantiated by discussing a parallel in how we have historically nurtured innovative airpower advocates and leaders. I also describe an existing Air Force graduate education program that largely meets the defined need, explore its potential downsides, and describe how this proposal fits into the ongoing efforts to develop a cyber warfare force. I finish with courses of action and a recommendation.

The three main components of this research seem to stand alone, but are linked through the wide array of AF cyber warfare organize, train, and equip efforts currently in progress. They all draw heavily upon my experience in supporting, researching, and teaching cyber warfare as well as my participation in the ongoing cyber force development efforts.

Projects such as this are never the work of one person. I would like to thank several groups that have supported me over the last several months. My fellow students have been a terrific source of inspiration. We have had great discussions, fierce arguments over philosophies, and much fun. I would also like to thank the ACSC faculty for their support. In particular, Col (ret) Roger Philipsek, Lt Col Michael Linschoten, and Dr. John T. LaSaine have been particularly helpful and encouraging. Maj Ray Simmons did me the favor of reminding me that while confidence is good, hubris and complacency have no place in a professional officer's toolbox. While most of the ideas expressed herein build upon the work of many people, any mistakes are mine alone.

I would like to offer special thanks to my wife and children for putting up with yet another round of schooling, and for moving twice in two years…

Finally, to the Reader:

If you are already a cyber operator, please bounce my ideas off your own, and let's talk! Collectively, we have a chance to shape where the AF/Joint Community ends up in terms of cyberspace warfare in the future. Collaborative effort expended now in defining a first-rate strategic vision for the future will pay huge dividends later for our national security.

If you are a communicator, you will be a cyber operator soon, so see the note above. I ask, however, that you note that my focus is primarily on the attack, defense, and exploitation aspects of cyberspace operations. Network creation and sustainment are indeed important components of cyberspace operations, but we are already good at them. Our ability to prosecute network warfare is still nascent, and your insights will be crucial as we proceed.

If you are new to cyber, you are really the person I'm trying to reach! I hope that this paper will give you a sense for the promise of cyber warfare, how it will help the AF protect our national interests, and why it is important that we take on this challenge. I also hope that you will become a cyber advocate!

To all Readers, I thank you for taking the time to peruse this paper! My goal has been to share a developing vision for AF cyberspace development, and your attention is helping realize that goal.

Abstract

Two significant and interrelated problems are hindering the Air Force's development of cyber warfare capabilities. The first is a lack of awareness about why the AF has chosen to take cyber warfare on as a core capability on par with air and space. The second stems from the lack of a commonly understood vision for how future AF cyber warfighting capabilities will support our national security objectives. This research project addressed these problems by exploring the following questions:

- *What types and ranges of offensive and defensive cyber effects might the Air Force provide, both externally for the combatant commanders and internally for self-defense, in the near and medium term futures?*
- *How should the Air Force develop and make those capabilities available to combatant commanders and internally?*
- *How might the Air Force nurture the cyber-oriented leaders who will envision and build the cyber capabilities needed in the future?*

The contributions of this research include a strategic vision for future cyber warfare capabilities that support both the combatant commanders and internal service needs. It also introduces a means of developing cyber warrior-scholars who will shape the cyber warfare domain of the future.

The vision for future capabilities is expressed through a set of vignette/discussion pairs. In "a Day in the Life" prose form, each vignette describes a situation and how the forces involved in the scenario handle the situation. An analysis of the people, processes and technology of each vignette evaluates how the services may organize, train, and equip to produce the required capabilities.

The cyber warrior-scholar concept is amplified by discussing how we develop advanced strategists and airpower advocates, including description of an existing Air Force graduate education program that largely meets the defined need, explores potential downsides, describes how this proposal fits into the ongoing cyber warfare force development effort, and finishes with courses of action and a recommendation.

Strategy can be thought of as defining a vision of the future, and mapping out how to get there. The overall goal of this research is to spur thought about what the vision for AF cyber warfare capabilities should look like, and drive discussion about how to make that vision a reality.

1 Introduction

The Air Force (AF), Department of Defense (DOD), and broader civil-military community is aware the AF and other services have designated cyberspace as a warfighting domain. However, what that actually means is not necessarily clear, creating friction and slowing the transformation of the AF into an Air, Space, and Cyberspace Force. The AF has proactively tackled the organizational and force management issues involved in developing our cyber warfighting capabilities, and has done much to spread awareness of these efforts. However, the capabilities and range of effects our new force and organizational structure will provide largely remain shrouded from popular view. This results in a lack of awareness about why the AF is tackling this mission. Additionally, there exists a popular perception that we have been talking about how to train and organize forces to fight with a weapon system that has not been defined. To a considerable degree, this is true—cyber warfare is a relatively new domain, and the AF has not yet determined how to wage war in and through cyberspace. In a very real sense, we are facing a set of challenges that would feel quite familiar to early airpower leaders such as Billy Mitchell, Pete Quesada, and George Kenney. Cyber power is as nascent as airpower was just prior to World War II, and we need to develop the innovative leaders and warriors who can envision and then shape the cyber capabilities of our future AF.

The goal of this research project is to assist the AF in its transformation into a force that fully integrates a full spectrum of integrated and interdependent kinetic and non-kinetic effects in support of the warfighting commanders. Towards that goal, this project describes a vision for the future in which a fully developed cyber warfare capability supports, and is supported by, the use of the air, space, land and sea weapons in holding our adversaries at risk in cyberspace while preserving our own freedom of maneuver. The factors above lead to the following research questions. *What types and ranges of offensive and defensive cyber effects might the AF provide, both externally for the combatant commanders and internally for self-defense, in the near and medium term futures? How should the AF develop and make those capabilities available to combatant commanders and internally? How might the AF nurture the cyber-oriented leaders who will envision and build the cyber capabilities needed in the future?* These questions shape the following research hypothesis and supporting goal.

Research Hypothesis: *Transformation to an Air, Space, and Cyber force requires total force awareness of how the AF, in conjunction with Air and Space, can fly, fight, and win in Cyberspace.*

Research Goal: *Provide a vision for cyber warfare capabilities that will benefit the combatant commanders as well as provide and protect the AF's garrison infrastructure, and describe a roadmap outlining how the AF can make the vision a reality.*

The impetus for this research project is raising strategic awareness of cyber warfare across the AF and joint communities. As discussed above, the problems involve both a lack of understanding of cyber warfare as a warfighting domain, and to some degree, a lack of strategic vision for how cyber warfare may benefit US national security in the near future. The problem/solution research methodology used herein addresses these problems by presenting a recommendation in the form of a vision for future cyber warfare capabilities, how they may be employed, and how the AF might organize, train, and equip (OT&E) our cyber forces to realize that vision. The target audience for this research include three main groups both inside and outside the AF community: those interested individuals who want to know how the AF cyber capabilities may operate in the near future, those skeptics who do not see a need for innovation and change in this area, and finally, the people who do not yet understand that cyber capabilities will greatly enhance the AF's ability to support national security objectives. Three specific targets include the rated, intelligence, and communications and information communities.

The paper progresses as follows:

Chapter 2, The Need for Transformation, is motivational in nature. It discusses the imperatives behind the shift from a communications-oriented force to a cyber warfare-oriented force. It also addressed some of the common questions people have about why the AF is embarking on this path.

Chapter 3, A Vision of Future USAF Cyber Warfare, expresses a vision for future capabilities through a set of vignette/discussion pairs. Each vignette describes, in "a Day in the Life" prose form, a situation, and how the forces involved in the scenario handle the situation. The vignette is followed by discussion in which the people, processes and technology from the vignette are analyzed in terms of how the services may organize, train, and equip to produce the required capabilities. Due to page length limitations, only two abbreviated vignettes are in Chapter 3; the complete vignettes are in Appendix A.

Chapter 4, Cyber ACTS/SAASS, combines the need for strategic vision with training by introducing a concept for developing cyber warrior-scholars. The concept is fleshed out by discussing how we develop advanced strategists and airpower advocates, describes an existing Air Force graduate education program which largely fits the bill, explores potential downsides, describes how this proposal fits into the ongoing cyber warfare force development effort, and finishes with courses of action and a recommendation. Again, due to page length limitations, the full argument for Cyber ACTS/SAASS is in Appendix B.

Chapter 5, Conclusion, wraps up the project by tying the three main components together, and advocating future research needs.

2 The Need for Transformation

This chapter addresses some of the common questions posed by people outside the cyber warfare (CW) force community along the lines of "Why do we need a new CW community?" or "How will an AF CW capability support the joint force commander (JFC)?". It begins with a discussion of why we need a new family of AF warriors (officer, enlisted, and civilian). Emphasizing the differences between future cyber operations and existing communications operations ties the new cyber warrior to the old. For many, information operations (IO) and cyber warfare seem synonymous, but they are not. This research discusses some of the factors differentiating IO and CW as well as the scope of cyber warfare. Why the new focus on CW should prove more successful than our foray into IO finishes the chapter.

2.1 Why do we need a new cyber warfare force?

This is a question the AF has been grappling with as a community for nearly two years, and like most great questions, the answer is both simple and complex. The simple answer is that some aspects of cyber warfare have been performed by AF warriors who's primary career fields have loaned them to that mission in a "pick-up game" capacity. For example, the AF has many outstanding officers, enlisted and civilian Airmen serving in both offensive and defensive network warfare roles. They are essentially on loan from their primary career fields for an assignment or two, and then our personnel center pulls them out of network warfare and places them back into their traditional duties. Due to the difficulty and complexity of the duties they perform, they may take up to two years to become proficient in their jobs. As a result, these on-loan warriors really only provide one year of fully qualified service before they are replaced by someone who must then be trained, thus repeating the cycle. When network warfare was only a small part of the AF's mission, this paradigm was acceptable; however, the changes taking place both internally and externally to the AF require a more concerted and professional approach to creating and maintaining a cadre of cyberspace warriors.

The more complex answer requires that we step back from what we already do well, communications, and move towards the new vantage point provided by the former Secretary of the Air Force Wynn and Chief of Staff Gen Mosley's addition of Cyberspace to the AF's warfighting domains.[1] From here, we see that the capabilities the nation needs from cyber warfare personnel in the future differ dramatically from our current strengths. "Flying and Fighting" in cyberspace requires that we develop cyberspace capabilities which extend the Air Force's global vigilance, reach, and power into areas outside our information technology (IT) domain. This entails:

- **Establishing the domain**—cyberspace is a man-made domain that differs significantly from other domains such as land, sea and air that exist independently of human activities. For example, cell phones will not work without their infrastructure, that includes cell towers with radio transceivers that connect into the wired telephone networks. Air traffic control systems cannot work without a network of integrated airfield and long range radars connected to communication and control centers scattered across the globe.
- **Controlling the domain**—attacking an adversary's resources in and through cyberspace as well as defending our own resources and ability to operate in cyberspace.
- **Using the domain**—cyberspace warfighting. It includes our use of information and information systems to enhance and support Air, Land, Sea and Space operations. It also entails influencing an adversary through integrated cyber and kinetic attack operations.

2.2 Moving towards Cyber as a Warfighting Domain

The AF's cyber warriors today focus on narrow subsets of cyberspace, attacking and defending Internet Protocol (IP) networks, and using electronic warfare (EW) against airpower-oriented targets. Future cyber warfare forces will need the capability to attack and defend a much richer set of targets, including critical infrastructure, such as power generation and distribution, fuel refining and distribution, water systems and more. Section 2.4 discusses the range of networks in more depth. Another example is DOD's growing unmanned aerial system (UAS) infrastructure. As Secretary of Defense Gates pointed out in a 2008 talk at Air University, the DOD is using more UASs, both for intelligence gathering and combat missions and this trend is going to continue.[2] This will require the protection of the portions of cyberspace needed to command and control (C^2) those vehicles—a critical role for our cyber defense forces. Even with manned aircraft, the protection of the airborne C^2 networks in a contested and degraded cyber environment is crucial. Moreover, while we defend our own C^2 capabilities we will seek to deny that same capability from intelligent and capable adversaries. These examples only represent the tip of the iceberg; the list of required warfighting capabilities will be lengthy and complex.

The combatant commanders, in conjunction with the services, will plan for and execute those capabilities, and in doing so will uncover new cyber warfare needs and requirements. While these new warfighting capabilities will include technological advances, the most important element will be the warriors who use the new capabilities in protecting our nation's interests.

So, given that we need a new family of cyber warriors, how can the AF go about developing them? The AF Roadmap for the Development of Cyberspace Professionals, signed into effect 6 Apr 2008 by Secretary Wynn, describes how we will build that force.[3] In short, this development effort will cultivate an operational, warfighting mentality in full-spectrum cyber professionals. These professionals will understand the cyberspace domain and will be capable of delivering offensive and defensive cyber capabilities, seamlessly integrated with non-cyber capabilities, across all warfighting domains, Air, Land, Sea, Space, and Cyber.

In addition to the offensive and defensive capabilities, a transformed set of capabilities built upon the foundation provided by our current communication and information (C&I) forces will establish the cyber domain. It is important to note the AF is not just redressing the C&I forces—it is transforming an entire culture that has historically provided support capabilities to one that focuses on delivering a full range of operational combat effects.

New capabilities will require flexibility for leaders to develop new tactics, techniques, and procedures (TTP) and doctrine in conjunction with research, tech developers, and operators. Some of the development can proceed through normal AF processes; however, given the newness of the domain, cyber warfare leaders will need to perform some capability and TTP development in the heat of battle. To enhance this process, the AF must provide a holistic education that includes broad understanding of theory and provides problem-solving skills, training in a variety of weapon systems, operational experience, and a solid understanding of how the joint fight takes place. Creativity and problem solving skills will be important characteristics of the future cyber leaders, whether they are joint force planners, researchers, operators in the field, or serving in a service staff. The cyber schoolhouses must become laboratories where Airmen can conceptualize and develop new warfighting capabilities as they train on the current state of the art. There is precedent for this concept in the Army Air Corp Tactical School (ACTS). See Chapter 4 for a concept of how we may develop appropriately educated cyber warfare leaders in a manner similar to how the Army Air Corp developed the generations of Airpower experts.

2.3 How does Cyber Warfare differ from Information Operations?

As discussed above, the development of cyber warfare capabilities and warriors will enable movement towards cyber as a warfighting domain. Nearly as important is for the cyber warfare community to distinguish their new capabilities from those currently labeled Information

Operations. The need to distinguish CW and IO derives from two concerns: IO's integration into military operations has been problematic, and the breadth of IO is too much for any single warfighting community to manage competently. Gaining the trust of the Joint Force Commanders will require that the CW community focus on a well-defined core set of CW capabilities that solve JFC problems in a trustable, repeatable manner. While these CW capabilities will integrate with IO and kinetic operations, they do not make up the whole of IO. To explain the differences, the jointly approved definitions in JP 1-02, *DOD Dictionary of Military and Associated Terms*, provide a starting point for discussion. Simply put, joint doctrine currently defines cyberspace as:

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[4]

Cyberspace operations are defined as:

> The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.[5]

From this definition, computer network operations and its subcomponents are:

> Computer network operations — Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO.[6]
>
> Computer network attack — Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA.[7]
>
> Computer network defense — Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. Also called CND.[8]
>
> Computer network exploitation — Enabling operations and intelligence collection

> capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called CNE.[9]

In contrast, joint doctrine defines information operations as:

> The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.[10]

Thus, cyberspace warfare is simply the computer network operations component of information operations: CNA, CND, and CNE. Cyberspace warfare is not electronic warfare, psychological operations (PSYOPS), military deception (MILDEC), or operations security (OPSEC); however, it supports and is supported by these other capabilities and all others across the warfighting domains. In joint doctrine CO includes both CNO and network creation and sustainment (NetOps). Because NetOps is well understood, this research focuses primarily on CW, the CNO component of CO. Unless specifically indicated, CO and CW are used interchangeably.

From a definitional standpoint, the matter seems clear. Nevertheless, for many Airmen, Soldiers, and Sailors who have been in this fight for a long time, the lines between these seem very blurry. In many minds there seems to be little difference between IO and CO. There are a few reasons for this, but the primary one goes back to the overarching nature of IO and its inclusion of disparate capabilities and disciplines under an influence operations umbrella. Joint Publication 3-13, *Information Operations,* designates EW, CNO, PSYOPS, MILDEC, and OPSEC as core IO capabilities. It then defines these core capabilities as the principle means by which a JFC influences adversaries and other target audiences. Of particular interest in terms of clearing up the confusion between CO and IO is JP 3-13’s identification of PSYOPS, OPSEC, and MILDEC as a core set of military functions that have existed for centuries. EW and CNO are new disciplines and became part of the IO core only recently. [11] AF doctrine, on the other hand, designates influence operations (IFO), EW, and CNO as core IO capabilities. IFO in AF terms encompasses PSYOPS, MILDEC, and OPSEC.[12] This latter perspective on IO seems to make the most sense in terms of distinguishing IFO, which may be carried out through any of the warfighting domains, including kinetic warfare, from non-kinetic effects-achieving capabilities such as those provided by EW and CO.

Throughout time, warriors across the world have understood that warfare is ultimately a means of influencing people and their decisions. This influence is the core of Information Operations—we affect an adversary's decision-making process through the integrated employment of specific capabilities through all domains, including Air, Space, Land, Sea, and Cyberspace. Figure 1 illustrates this relationship. Here information operations make use of capabilities in all domains, including cyberspace, to influence a target audience or adversary.

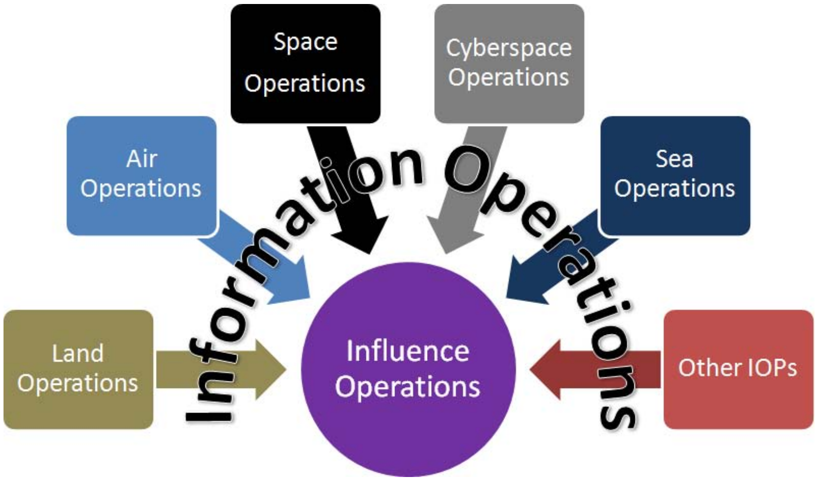

Figure 1: The relationship between warfighting operations, information operations, and adversary influence

Looked at this way, it is easy to see that the AF's development of cyberspace capabilities enhances the US military's ability to reach into an enemy's cyberspace and affect decision making processes while, at the same time, working to prevent them from affecting ours.

Cyberspace warfare operations both support and are supported by the other domains. Our new cyberspace doctrine, currently undergoing review, reflects this understanding.[13]

2.4 Changing the Scope and Focus of AF Cyber Warfare

Traditionally, AF network warfare forces, both offensive and defensive, have focused most of their efforts and capabilities on IP-based networks. IP networks comprise the most visible parts of cyberspace, and encompass the non-secure IP router network (NIPRNet), SECRET IP router network (SIPRNet), and other classified networks connecting administrative and command and control computers. Additionally, the range of warfighting capabilities targeting IP-based networks has been limited to a handful of offensive and defensive effects.[14] Given CW's origins in the communications and information domain, this IP-based administrative network emphasis made sense several years ago. Likewise, the nascent state of AF CW, the limited capabilities represented reasonable competency. However, as the new definition of cyberspace illustrates, cyberspace is much broader and more complex than just IP-based networks. Table **1** lists a sampling of networks that make up cyberspace.

Table 1: Example Networks in Cyberspace (adapted from Franz's work[15])

IP-based Communication Networks - Internet - NIPRNet, SIPRNet, etc. - Voice over IP (VOIP) telephony systems - Banking Infrastructure	Closed-network Battlefield Systems - Integrated Air Defense Systems (IADS) - Tactical Data Information Links (TADIL) - C^2 Networks
Distributed Control Systems - Supervisory Control and Data Acquisition/Control Systems (SCADA/CS) - Manufacturing Process Control Systems - Energy Generation and Distribution Systems	Tactical Communication Networks - Theater Airborne and Terrestrial Radio Systems - Mobile Radios (cell phones, mobile data services) - Land Mobile Radio (LMR) (first responder, law enforcement, local C2 networks)
Transportation Control Systems Regional or Global Air Traffic Control (ATC) Systems Airfield Air Traffic Control and Landing Systems (ATCALS)	Global Communications Networks - Satellite Communications Networks (SATCOM) - Fiber Optic Networks - Telephony - Global Positioning Systems

Supporting JFC requirements in the future will necessitate the development of attack, defense, and exploitation capabilities across the full range of networks in cyberspace.

Additionally, the services all have internal infrastructure defense needs that essentially span the same range of networks. For example, the heating and cooling, power distribution, and fuel distribution systems used on AF bases, both garrison and deployed are SCADA/CS systems. These networks are usually not thought of in terms of cyber defenses, but they are just as critical to base operations as are the communication systems. The main point of this section is that the range of capabilities required from future cyber forces is significantly larger and more complex than that of today.

2.5 Joint Integration (including Inter Agency)

Cyber operations are not unique to the AF. All services have internal defensive needs, and all services will offer cyber operations capabilities to the combatant commanders (CCDR). The question then becomes "Who provides what capabilities to the CCDRs?" Should the services all develop similar, overlapping capabilities, or does it make sense to define service specific rolls based upon the core service missions? For example, should the AF focus its efforts on cyber warfare capabilities that match its global strike and global reach capabilities? Should the Navy concentrate on the cyber aspects of seaport management, maritime communications, and maritime transportation infrastructure? Should the Army center its attention on land-based transportation systems, land-force-centric C^2 and other battlefield systems?

Whatever the answer to the proceeding questions, the entire cyber warfare community needs to come together in defending the US critical cyber infrastructure. What has largely been missing from public discussion about cyber is an effective active defense structure: the people, organizations, and partnerships that will pick up where the technological, passive cyber security measures including software, hardware, and policies leave off. This structure must include government (federal, state, and local), law enforcement (federal, state, and local), DOD (active, reserve, and National Guard), the commercial industrial base, and the common use cyber environment. We need to be able to develop and leverage intelligence about possible threats to any critical national cyber asset, not just military targets, and to monitor those threats for indications and warning of pending or ongoing attacks. We need to develop the ability to respond, proactively where possible, and reactively where needed, to the full range of cyber attacks. We must structure our defenses across the entire cyber-dependant community such that we can defend against the threats, and operate through those attacks we cannot prevent.

Unfortunately, many military personnel today think of cyber defense as an internal concern. The current DOD cyber defense focus is almost solely on our garrison infrastructure; we act as if that is the most important target and protecting it will ensure our warfighting capability. This perspective downplays our dependencies upon commercial infrastructure such as backbone networks and commercial transportation systems such as those relied upon by USTRANSCOM. We must look past today's traditional patterns of activity, our entrenched "lanes in the road" separating the military, law enforcement, and public and private critical infrastructure, and search for partnerships that will be effective against tomorrow's cyber threats.

This research paper contains a vision for the future in which a robust cyber attack, exploitation, and defense force takes the cyber fight to our enemies, while also actively protecting our cyber infrastructure. In this future, DOD active duty attack, exploitation, and defense capabilities work with and through DHS; the state National Guards; federal, state, and local law enforcement; and commercial industry to actively defend our nation's critical cyber infrastructure. One key to this future is coupling DOD's Title 10 and 50 authorities to the National Guard's Title 32 and 18 authorities, and their local connections to law enforcement and industry. Certainly, there are a lot of barriers and unresolved questions about how we should move forward in developing a national active defense capability, but move forward we must.

2.6 Why will this work better than what we have been doing?

First and foremost, most of it has not been done in the past! The discussion above highlights the fact that AF CO/IO forces have not actively defended networks other than NIPRNet/SIPRNet. Other parts of this, such as network defense, will be done better because the people responsible for defending our networks will have a thorough understanding of how networks are attacked—and our attackers will have that same level of understanding of the defensive mission. While the EW forces have focused on operations since inception, the warfare side of cyberspace was handled as a pickup game, with communicators and intelligence personnel "loaned" to the network attack and defense missions for an assignment or two and then pulled back into their primary duties. This resulted in little attack and defense depth across the force, thus leaving us vulnerable to attack and limiting our ability to leverage the offensive capabilities available in this new domain. By officially recognizing cyberspace as a warfighting domain, we enhance our ability to organize, train, and equip forces capable of achieving both offensive and defensive effects in areas crucial to our country.

An additional facet to this question stems from the array of network classes discussed in Section 2.4. The military maintains and uses all of the network classes, including those associated with infrastructure such as SCADA/CS, and needs to develop the ability to monitor and defend these network classes from attack. From an attack perspective, we need to develop the ability to attack those networks in potential adversarial countries, and recognize that our adversaries are doing the same for our critical infrastructure. The US currently treats cyber attacks against critical infrastructure targets as criminal acts, and the protection of these networks is not traditionally considered a military responsibility. There are many reasons for this. One of the most relevant is that most critical infrastructure is privately owned and operated, and none of the cyber attacks against this infrastructure have involved anything other than criminal acts (including espionage).

This leads to a second reason, which is that we have not yet had a nation-state declare war on the US and, under the auspices of that war, prosecute cyber attacks on our critical infrastructure. Enemy submarines launching cruise missiles from the Gulf of Mexico into coastal refineries would certainly draw a military response. It seems likely that a cyber attack capable of wreaking the same amount of destruction should also result in a military response; especially if it is possible to develop military capabilities to defend against such an attack. This is certainly a controversial topic, and while worthwhile, it will not be developed in this paper. However, it seems likely that an active and robust partnership between the active duty military, state national guards, Northern Command, the Department of Homeland Security, and industry will be needed to chart our way ahead in this domain. One possibility that is explored in Chapter 3 uses a combination of active duty and National Guard cyber forces to respond to a cyber attack against US critical infrastructure.

2.7 Wrapping up the Need for Transformation

This chapter provided motivation for why the AF and other services need to develop cyber warfare capabilities, and answered some of the common questions people have about why the AF has embarked on this path. In doing so, it introduced the new cyber warfare force, and discussed why cyber as a warfighting domain differs from communications. It distinguished cyber operations from information operations, and described the expanded range of networks AF cyber capabilities need to effect. The need for joint and interagency integration, and why what the AF is doing now is an improvement over the past wrap up the chapter. The next chapter concentrates on developing a vision for future AF and joint cyber warfare capabilities.

3 A Vision of Future USAF Cyber Warfare

This chapter builds upon the call for transformation presented in Chapter 2. It provides a strategic vision for how the AF and other services may organize, train, and equip cyber warfare capabilities over the next few years. It also envisions and discusses how the combatant commanders may use these forces. Overall, the nation needs a robust cyber attack, exploitation, and defense force capable of taking the cyber fight to our enemies, while also actively protecting our cyber infrastructure. In this future, DOD active duty attack, exploitation, and defense capabilities work with and through DHS; the state National Guards; federal, state, and local law enforcement; and commercial industry to actively defend our nation's critical cyber infrastructure. The primary focus of this chapter is cyber operations as defined in Section 2.3: computer network attack and defense. Network operations certainly play a role, but the main emphasis is on warfighting versus sustainment.

3.1 Structure

The vision below and augmented by material in 0, is expressed through a set of vignette/discussion pairs. Each vignette describes, in "a Day in the Life" prose form, a situation, and how the forces involved in the scenario handle the situation. The vignette is followed by discussion in which the people, processes, and technology from the vignette are analyzed in terms of how the services may organize, train, and equip to produce the required capabilities. Due to space limitations, Chapter 3 contains only two vignettes, and those are in abbreviated, summary form. For the full stories and analysis, see 0. These vignettes represent only a partial vision, much work remains in describing a holistic future capability.

Table **2** summarizes the various vignettes. These vignettes represent only a partial vision, much work remains in describing a holistic future capability.

Table 2: Vignette Descriptions

Name and location of Vignette	Summary
Two Futures: Part 1—Today Summarized in Section 3.2, full text in Section A.1	An adversary uses a multi-front, asymmetrical cyber attack to distract the US and prevent a military response to an act of aggression in yet another theater. The US response, using today's capabilities and hobbled by today's disadvantages, is disjointed and, in the end, inadequate.
Two Futures: Part 2—Tomorrow Summarized in Section 3.3, full text in Section A.6	The same scenario as Part 1—Today, but using the envisioned cyber warfare capabilities possible in the near future and results in a different outcome.
Unit-level Cyber Training Full text in Section A.2	Addresses current shortfalls in cyber training and exercise capabilities at the unit level. Introduces inexpensive, network simulation environment capable of providing realistic training. Emphasizes training communicators to handle contingencies to supported missions.
Base-level Red-teaming Full text in Section A.3	Continuous cyber red-teaming at the base level exposes the defenders and maintainers of cyber infrastructure to simulated combat situations. This exposure forces the exercising of warfighting skills, helps identify weaknesses and vulnerabilities, and enhances unit performance actual combat operations.
CNE by base-level attack personnel Full text in Section A.4	Addresses two shortfalls in the DOD; there are too few cyber intelligence-gathering assets, and maintaining currency in cyber attack for our offensive cyber forces is difficult. Because CNE and CNA are very similar, using cyber attack forces at the unit level in cyber exploitation missions affords them a means of maintaining currency and at the same time satisfies AF and DOD exploitation requirements.
Integrated Operations Full text in Section A.5	Traditionally, cyber warfare operations were distinct from traditional kinetic operations. In the future, well developed and integrated cyber operations will support and be supported by land-based and airborne operations.

The vignettes are entirely fictional, are drawn from the author's imagination, and do not reflect real people, organizations, or conflicts. While real nation states are used, the goal is not to insinuate that a particular nation would act in the manner depicted, but rather to highlight how publically known cyber warfare capabilities that nation possesses may be used. Likewise, the associated analyses are intended to spur discussion, not reflect policy, particularly concerning international relations.

3.2 Two Futures: Part 1—Today

This vignette highlights one of many potential threat scenarios the US and allies may face today. In it, an adversary uses a multi-front, asymmetrical cyber attack to distract the US and prevent a military response to an act of aggression in yet another theater. The US response, using today's capabilities and hobbled by today's disadvantages, is disjointed and, in the end, inadequate. The adversary wins this round.

3.2.1 **Abbreviated Vignette** See Section A.1.1 for the full vignette.

1. China forces a confrontation between Russian and US forces in the Gulf of Aden.
2. As this heats up, China, using botnets thought to belong to Russian cyber forces, attacks select parts of America's critical infrastructure.
3. Using cyber compromise of an American destroyer's weapon system, they remotely fire American weapons and sink a Russian frigate. The Russians shoot back…
4. The Chinese then unleash a wave of network attacks against Russian critical infrastructure from compromised machines in America. At the same time they extend the attack against America's infrastructure using compromised machines in Russia to paralyze the movement of transportation in America.
5. The American President attempts to call the Russian Prime Minister, but all commercial communications into and out of the United States are overwhelmed by the ongoing cyber attacks. He resorts to using the Cold War teletype system, and the two leaders assure each other that they did not authorize any part of the ongoing and escalating fighting. Both sides agree to call for immediate cease-fires, and agree to keep nuclear forces at low levels of readiness.

6. China CW forces, deeply entrenched in both American and Russian command and control systems, intercept the outgoing cease-fire orders and modify them. Some units are directed to higher levels of readiness and/or are given attack orders, while others are told to stand down or redeploy. Confusion reigns. The compromise of the networked C2 systems is rapidly detected, and very quickly, personnel no longer trust information flowing up, down, or laterally throughout the DOD or Russian equivalent organizations.
7. While all this is happening, Chinese Special Forces have captured Taiwan's leadership and moved them to mainland China. At the same time, they destroy Taiwan's communications links off the island and jam all satellite communications. Dozens of commercial freighters, which had been moving into Taiwan's harbors over the last couple of days, docked and offloaded PLA mechanized and infantry forces. Within hours, they have taken Taiwan, almost without firing a shot. America, tied up in the instigated fight with Russia, has not even noticed.
8. The Chinese CW forces back out of both America and Russia's networks, destroying all data they could reach as they go.
9. In the aftermath, the Americans and Russians realize what happened, but China left almost no traces of the attacks, and denies all involvement.

3.2.2 **Abbreviated Discussion** See Section A.6.2 for the full discussion.

China has well developed and integrated CNA forces.[16] They have conducted extensive intelligence preparation of the battlespace (IPB) in terms of DOD, Defense Industrial Base, and commercial and public critical infrastructure.[17] China's CNA forces have very likely embedded stealthy attack capabilities in our military and civilian networks via supply chain attacks, have prepared large botnets to use as attack platforms, and have waves of computer viruses prepared to unleash against us.

The supply chain attack mentioned above represents one the gravest risks the US and other technological forces face today. For example, most computing architectures, including those used in weapon and C^2 systems use integrated circuit components and associated software that are developed and produced in untrusted environments. Today's best defensive technology is unable to detect if such devices are compromised, or how they may behave if implanted capabilities are triggered.

Conficker, a self-spreading worm in the news recently[18], highlights a pedagogical cyber threat—the armies of compromised networked computers known as botnets. At the time of this writing, the Conficker botnet is estimated at 15 million computers.[19] It is also responsible for crippling military C^2 systems, thus grounding French fighter aircraft. It has also affected British aircraft and naval vessels, including the aircraft carrier Ark Royal.[20] This type of threat is clearly of concern to any modern military.

An enormous amount of damage can be done with botnets. For examples, ask the Estonians[21], or the Georgians[22]. Both countries have suffered crippling cyber attacks in recent years from botnets possibly controlled by Russian sources. Distributed denial of service can be so overwhelming that little can be done about them except to shut off external Internet connectivity to the attacked systems. This strategy will not work for the US, or even the US military. We are too connected and dependent upon external connections to isolate ourselves and continue to operate effectively.

This scenario is representative of an asymmetric and limited cyber war prosecuted by an adversary hoping to keep our conventional military out of some fight. In preparation of an attack against US interests by a cyber-equipped adversary such as China, we can expect their cyber warfare forces to attempt to achieve the following effects:

1. Distract the populace, government, and military by causing problems at in the US, in our allies' countries, and/or in other theaters of operations. The intended effects would be mass panic and confusion across domestic populace. They would use non-destructive means and count on this type of cyber attack having short-lived effects, and not causing long-lasting damage which might cause the US and allies to retaliate against their homeland using weapons of mass destruction (WMD.)
2. Slow down or prevent our deployment of forces to a regional conflict. They would do so by attacking TRANSCOM and its supporting civilian infrastructure. This type of attack may be more lasting than that against the civilian infrastructure.
3. Disrupt our military command, control, and communications (C^3) infrastructure. They would accomplish this by shutting down the network backbones upon which NIPRNet, SIPRNet, and other networks ride. This type of attack may also be more lasting than that against the civilian infrastructure.

As discouraging as it may be, the US and our allies are probably more vulnerable to the type of threat scenario described than any other countries. At a strategic level, we lack an effective means of detecting coordinated attacks across military, governmental, critical infrastructure, and private cyberspace. Nor do we have appropriate mechanisms in place to counter such an attack, or let us operate through it.

This vignette and discussion, Two Futures: Part 1, are intended to paint an uncomfortable picture of a realistic threat coupled with our current inability to counter that threat. They represent the state of today's cyber warfare competence. See Section 3.3, Two Futures: Part 2, for how different the outcome may be if the AF and rest of the US cyber community develop a robust cyber warfare capability.

3.3 Two Futures: Part 2—Tomorrow

The conflict in Part 1—Today did not go so well for the US or our allies, in part because we were not ready to handle the type of cyber warfare even a modestly competent adversary could throw at us. Some of the problem had to do with internal military defense needs, some was a lack of appropriate intelligence capabilities, but a lot had to do with the lack of partnerships between military, government, and private cyber infrastructure and defense capabilities. The vignettes and associated discussion contained in this chapter and Appendix A present a partial vision for how we may organize, train, and equip our cyber forces in the near future. The vignette below takes advantage of the envisioned capabilities, and results in a different outcome to the same type of attack.

3.3.1 **Abbreviated Vignette** See Section A.6.1 for the full vignette.

1. Intel forces identify both the Russian and US botnets as they are constructed, possibly co-opting them for friendly use. In addition, botnets are monitored for indications and warning (I&W). Supply chain attacks are mitigated by a combination of engineering and operational measures. Essentially, we acknowledge that we cannot guarantee security, engineer systems to operate correctly even when under attack, and exercise the ability to function in a contested and degraded cyber environment.
2. Robust defenses thwart initial Chinese attack against US C^2 systems. We also detect the attacks against Russian C^2, inform the Russians, and potentially help them defeat attack. Alternatively, they help us.

3. The targeted and distributed denial of service (DDOS) attacks against US infrastructure are detected and thwarted by an interagency cyber defense capability involving active duty intelligence, National Guard cyber warriors, DHS, law enforcement, and industry.
4. Ultimately, the intent behind the Chinese attack is detected, Taiwan is warned, the US is able to mobilize in time to stop the invasion, and the Chinese plan is defeated.

3.3.2 **Abbreviated Discussion** See Section A.6.2 for the full discussion.

The cyber research and development community has known for many years that no information system will ever be invulnerable to attack. Therefore, the emphasis for security must concentrate on engineering systems capable of operating correctly through attacks. We must exercise operating in contested and degraded environments such as those we are likely to face in real world situations. Our focus must cover the entire interdependent cyber infrastructure, not just military or civilian stovepipes. Capabilities such as red-teams, active defense forces, and well thought out and supported connections between the various aspects of our cyber infrastructure will enhance technological improvements in dramatically improving our overall cyber security.

3.4 Wrapping up the Vision

This chapter has summarized a series of vignettes that paint a picture of how future cyber forces may be organized, trained, equipped, and employed. Each vignette was coupled with analysis of the scenario as applied to the development of a roadmap for the future.

One can argue that the first vignette was overly pessimistic, and that the last one is overly optimistic. This may be true, but it may not as well. Our world is increasingly dependent upon cyberspace, and this dependence brings both promise and perils. Neither is well understood, and it will take a new breed of leaders to guide us into the future. The following chapter and Appendix B discuss one possible methodology for developing such leaders.

4 Cyber ACTS/SAASS

At the dawn of Airpower, the Army Air Corps created the Air Corps Tactical School—a school focused upon developing tactics, techniques, procedures, and doctrine about how to best use airpower in war. Currently, the AF School for Advanced Air and Space Studies (SAASS) grows highly capable warfare strategists in support of the joint fight. We need to blend ideas from these two programs into a school that grows cyber power leaders capable of guiding the AF into a future in which we can fly, fight, and win in air, space, and cyberspace in support of America's military objectives. This chapter summarizes the main arguments for the creation of such a program, and provides a recommended course of action. This concept is fleshed out by discussing in parallel how we develop advanced strategists and airpower advocates, describes an existing AF graduate education program which largely fits the bill, explores potential downsides, and describes how this proposal fits into the ongoing cyber warfare force development effort. See Appendix B for a full analysis and several alternative courses of action.

4.1 Problem Statement and Introduction

In many ways, cyber warfare is in its "Billy Mitchell" days, analogous to the advent of airpower prior to World War II. We are aware of potential and actual risks in this new domain but do not fully understand them. Just as the ACTS was the birthplace of modern airpower, we need a school which develops cyber-oriented warrior-scholars who can help guide the AF through its transformation into a force capable of flying, fighting and winning…in air space, and cyberspace. One possible means to develop such leaders is to add a second year of technical study of the cyber domain to the operational art and science foundation provided by Air Command and Staff College (ACSC). The second year Cyber School already exists within Air University; it is the Intermediate Developmental Education (IDE) Cyber Warfare program at the

Air Force Institute of Technology (AFIT).[23] The AF should create a two-year professional military education (PME) path consisting of ACSC followed by AFIT's Cyber Warfare program, to parallel the current path of ACSC followed by the SAASS.

To understand why we need a new cyber-focused educational program, consider as a starting point the distinction between education and training. Air Force Doctrine Document 1-1, *Leadership and Force Development*, describes the difference as follows,

> Education provides critical thinking skills, encouraging exploration into unknown areas and creative problem solving. Its greatest benefit comes in unknown situations or new challenges. Thus, education prepares the individual for unpredictable scenarios. Conversely, training is focused on a structured skill set, and the results of training performance should be consistent. Thus, training provides the individual with skill expertise. Education and training together provide the tools for developing Airmen.[24]

The current Air Force and DOD methodology for developing cyber warfare forces, including the future leaders in this domain, is heavily focused on training instead of education. Fundamentally, operations in a new warfighting domain such as cyberspace take place in a fog of uncertainty, full of unknowns and new challenges. Most people in the AF and other services have very little idea what exactly cyber warfare brings to their own mission, much less the joint warfighting environment.

Inside the AF, it is difficult to develop advocacy for as yet undeveloped and unproven cyber capabilities, forces, and organizations, given that supporting cyber capability development means not supporting some other proven capability. Externally, because we do not yet have much to offer the JFC in terms of trustable, usable cyber warfighting capability, it is difficult for the JFC to articulate requirements for capabilities the services can then provide, much less plan for their use in combat.

How do we address these problems? We start with an understanding of the effects needed by the JFC in current and near future conflicts, and the capabilities provided by existing kinetic warfighting capabilities. This is knowledge that many "operators", or warfighters, in today's AF possess, but which is not as well understood by the developing cyber warfare force and supporting science and engineering community. Equally important is awareness of today's cyber warfare technological capabilities, and where cyber capability development has the potential to go in the near future. This knowledge is primarily possessed by a handful of scientists and engineers. A leadership-oriented education program combining both sets of understanding and focusing on creative thinking and problem solving will produce highly innovative, technically competent warfighters. These officers will be able to lead the fight, identify needed improvements or new effects, and work with the research and development communities to produce new warfighting capabilities.

4.2 What is the value in a second year school?

Air University's SAASS is the AF's second year graduate school focused on developing strategists and warrior-scholars who possess superior abilities to develop, evaluate, and employ airpower in conjunction with land and sea capabilities in complex warfighting environments.[25] Its predecessor, the School for Advanced Airpower Studies (SAAS) was created in 1988 primarily to develop strategists.[26] The Air Force re-designated SAAS as SAASS in 2002.

The Army's School of Advanced Military Studies, the Naval Operational Planners Course, and the Marine Corps' School of Advanced Warfighting are equivalent programs intended to develop advanced warfighters in their respective services.[27] The Joint Advanced Warfighting School focuses on developing advanced campaign planners and strategists for the Joint Staff and combatant commands.[28] All three service-schools build upon an operationally focused foundation provided by first year graduate studies in the Air Force's Air Command and

Staff College, the Army's Command and General Staff College, and the Marine Corps' Command and Staff College residence programs.

Graduates from all four advanced service schools have been some of the most influential strategists and leaders in their domains. They are able to leverage a broad understanding of the art of war and the dynamically evolving capabilities of our military forces into strategies that prove effective against our enemies. The model of enhancing the broad warfighting backgrounds provided to in-residence IDE graduates with advanced education in a particular area is very attractive in terms of growing influential and effective leaders who possess both depth in their warfighting domains and breadth in terms of how to support the joint force commander in achieving operational and strategic objectives.

4.3 What is AFIT's IDE Cyber Warfare Program?

AFIT developed the IDE Cyber Warfare (ICW) program to support the handful of IDE students sent to AFIT in lieu of the in-residence ACSC program. A one-year program culminating in a Master of Cyber Warfare degree, ICW develops technical and leadership proficiency in both CW and CO, with emphasis on the operational and strategic levels of war. The curriculum emphasizes education and research into both offensive and defensive CW operations. Ultimately, it develops cyber warfare proponents who understand and can articulate how best to apply cyber power in achieving military objectives. While ICW is cyber-focused, the curriculum's foundations include the full spectrum of IO as defined by joint doctrine.[29]

4.4 Whom and how many should the USAF send to ICW after ACSC?

A centralized process should competitively select officers from a pool of volunteers. While all first-year residence school graduates should be eligible, the main goal of this program is to develop cyber-power advocates who will lead the cyber warfare forces in developing cyber capabilities in support of JFC objectives. Thus, emphasis should be on officers who will likely lead cyber units, integrate cyber into the planning process, or act as cyber advocates on joint and service staffs. Air Force Specialty Code (AFSC) 33S communications, 14N intelligence, 11X pilots, 13S space and missile operations, and 12X electronic warfare/navigator officers and their sister service peers would be the most likely prospects for attending such a program.[30] An initial cadre of 15 to 20 cyber-oriented warrior-scholars, able to bring to the fight both the operational breadth provided by the in-residence IDE and the technological depth provided by ICW, will be a powerful force for development of cyber capabilities in support of the joint fight. While this discussion is AF-centric, the cyber fight is joint and interagency, and as such, programs such as this should be open to all future leaders in cyberspace warfare.

4.5 What are the downsides?

The Air Force has too few officers in the field already. Having officers in school for an additional year represents a significant burden. There are also management and Permanent Change of Station (PCS) costs to consider, a significant issue in today's budget-constrained environment. These are real costs and cannot be downplayed; however, they represent an investment in the Air Force's cyber capability that will pay substantial dividends. Fortunately, AFIT has sufficient capacity to absorb 15-20 additional ICW students. Therefore, the majority of the programmatic costs will be management overhead and PCS expenses.

4.6 Cyber ACTS/SAASS Recommendation and Conclusion

The AF should establish a new Air Force program dedicated to developing cyber-oriented warrior-scholars. This program would parallel the ACSC to SAASS program, and consist of the resident ACSC program at Maxwell AFB followed by the resident AFIT ICW program at Wright Patterson AFB. Students would be competitively chosen from the 11X, 12X, 13S, 14N, and 33X AFSC in-residence school graduates, and placed in key positions after program completion.[31] Program timelines would match those of ACSC/SAASS.

Pros: The graduates from this program would have an in-depth understanding of the operational art of war and employment of airpower from ACSC, and an in-depth understanding of cyber warfare and how to create cyber power from AFIT's ICW. They would be both technically and operationally proficient, which would enable them to provide the innovative thought needed to develop cyber power as a warfighting function, as well as be respected and influential leaders of the cyberspace forces. Because their selection for in-residence school has already identified them as likely future senior leaders, they are more likely than average to be placed in key positions following the program. Finally, ACSC teaches officers how to use airpower to fight and win at the operational level of war. The cyber education from AFIT's ICW would enable the cyber power advocates to integrate both kinetic and non-kinetic capabilities across the warfighting spectrum.

Cons: The primary downside to this course of action (COA) is cost. Officers in the program are out of the fight for two years, and it would involve two PCSs - one to ACSC and another to AFIT.

This may not need to be a permanent program—the Air Force's abilities to fly, fight, and win in cyberspace will likely solidify into mainstream processes in ten to fifteen years. Until then we need to look back at how graduates of the Air Corp Tactical School and SAAS were able to make the most of the new capabilities airpower provided. Following this model will enable the Air Force to fully develop cyber power and enable its seamless integration into our warfighting capabilities. Just as all second year PME graduates have been influential in developing American warfighting power to its current heights, the ACSC/ICW graduates will be innovative, forward thinkers able to guide our Air Force towards a future in which we can counter all potential adversaries in all the domains in which we operate - air, space and cyberspace.

5 Conclusion

The AF is working hard to operationalize its capability to wage war in cyberspace; a new and difficult challenge. This research project explored three facets of the challenge: motivation for change to support cyber warfare, popular awareness of what AF CW may entail, and the development of cyber warfare leaders through appropriately focused education.

The motivational material in Chapter 2 discussed the imperatives behind the shift from a communications-oriented force to a cyber warfare-oriented force. In doing so, it addressed some of the common questions people have about why the AF is embarking on this path, differentiated IO from CO/CW, and finished with why the AF's new focus on CO is an improvement.

Chapter 3 and Appendix A extend the motivation from Chapter 2 with a vision for how the AF and other services may OT&E cyber forces for presentation to the CCDRs. A series of "Day in the life" vignettes express this vision as they portray a range of cyberspace operations. The vignettes are coupled with discussion about how the AF might organize, train, and equip a force to best achieve the capabilities described. The vignettes represent merely a starting point, many other are needed to fully explore and express a complete strategic vision.

The vision expressed in Chapter 3 represents one person's vision, but the AF's strategic direction will require the innovative perspectives of many visionaries. The essay summarized in Chapter 4 and extended in Appendix B introduces a concept for how and why the Air Force should develop cyber-oriented warrior-scholars capable of shaping the Air Force fight in cyberspace. This concept is substantiated by discussing how we have historically nurtured innovative airpower advocates and leaders. The AF already has a graduate education program that largely fits the bill. The essay explores the concept's potential downsides, and describes how this proposal fits into the ongoing cyber warfare force development effort. It finishes with courses of action and a recommendation.

Appendix A – Vision Continued

This appendix contains the full set of vignettes and discussion introduced in Chapter 3, A Vision of Future USAF Cyber Warfare.

A.1 Two Futures: Part 1—Today

This vignette highlights one of many potential threat scenarios the US and allies may face today. In it, an adversary uses a multi-front, asymmetrical cyber attack to distract the US and prevent a military response to an act of aggression in yet another theater. The US response, using today's capabilities and hobbled by today's disadvantages, is disjointed and, in the end, inadequate. The adversary wins this round.

A.1.1 Vignette

US and Russian naval forces are operating near each other in the Gulf of Aden off of Somalia on anti-piracy missions. Using a supply chain attack, Chinese cyber warfare forces have compromised the fire control systems on both an American destroyer and a Russian frigate, and have the ability to aim and fire them at will as soon as the weapons are placed on alert status. The Chinese People's Liberation Army (PLA) has placed a device that emits radioactivity simulating a small nuclear weapon on a Liberian freighter, and arranged for its capture by Somali pirates. Chinese Special Forces in Pakistan and Kenya near suspected al Qaeda locations engage in a lightly encrypted and highly charged satellite phone exchange about the "hijacked Fist of God." Both American and Russian signals intelligence (SIGINT) operations pick up the transmissions and rapidly decode them. The two militaries employ sensors capable of detecting the presence of the suspected bomb, and quickly identify the hijacked vessel as containing a suspected nuclear weapon. Both the Russian and America task groups dash toward the ship.

At the same time, Chinese CW forces have completed their preparations for a massive and sustained attack against America's critical infrastructure. Their extensive infiltration of DOD's networks over many years has yielded immense amounts of information about how the DOD operates. They used this information to highlight vulnerabilities, and crafted and implanted stealthy attack implants in crucial nodes of the DOD's warfighting command and control networks.

As the battle groups converge in the Gulf of Aden, China's cyber warfare forces prepare two large botnets for action against targets in the US and Russia. The first botnet was constructed primarily under contract by Russian organized crime organizations. Carefully selected information about parts of the botnet were leaked to the US intelligence sources in a MILDEC campaign, with the intent of leading the US to believe that the botnet was under Russian military control. Likewise, the Chinese leaked the existence of the second botnet to the Russian's by planting information about it that leads back to the US military.

China's CW forces selectively engage the first botnet in DDOS attacks against key parts of the USA's economic and transformation infrastructure. They specifically do not target news organizations. Their goal at this point is to draw America's attention inward, and away from what is happening elsewhere in the world. Because of an ongoing financial crisis, the attacks against the banking and stock markets are quickly picked up and broadcast through the media, causing a panic across the country. Just in case the US military did not catch that the attacks were coming from purportedly Russian botnets, comments to that effect are "leaked" to the press by Chinese psychological warfare forces and promulgated.

As the US and Russian battle groups close in on the hijacked ship, Chinese electronic warfare forces in that region begin jamming all radio communications. This prevents the US and

Russian forces from communicating. Concerned about what appears to be threatening behavior from the Russians, the US commander orders that weapons be trained on the Russian strike group and armed. The Chinese cyber warfare forces detect this at, and fire the US weapon systems, sinking a Russian frigate. The US commander shuts down his weapons as quickly as possible, but the damage is done. The Russians start shooting back and a major skirmish ensues.

At this point, the Chinese open up massive DDOS attacks against Russian critical infrastructure using the botnet thought to be under US control. At the same time, they extend the attack against US infrastructure to paralyze the movement of transportation in the US. They also selectively target key nodes in the backbone communication networks in the US, effectively cutting off all military and federal government communications as well as all wired and cell telephony in North America.

The American President attempts to call the Russian Prime Minister, but all commercial communications into and out of the United States are overwhelmed by the ongoing cyber attacks. He resorts to using the Cold War teletype system, and the two leaders assure each other that they did not authorize any part of the ongoing and escalating fighting. Both sides agree to call for immediate cease-fires, and agree to keep nuclear forces at low levels of readiness.

China CW forces, deeply entrenched in both American and Russian command and control systems, intercept the outgoing cease-fire orders and modify them. Some units are directed to higher levels of readiness and/or are given attack orders, while others are told to stand down or redeploy. Confusion reigns. The compromise of the networked C^2 systems is rapidly detected. As a result, personnel no longer trust information flowing up, down, or laterally throughout the DOD or Russian equivalent organizations.

While all this is happening, Chinese Special Forces have captured Taiwan's leadership and moved them to mainland China. At the same time, they destroy Taiwan's communications links off the island and jam all satellite communications. Dozens of commercial freighters, which had been moving into Taiwan's harbors over the last couple of days, docked and offloaded PLA mechanized and infantry forces. Within hours they have taken Taiwan, almost without firing a shot. America, tied up in the instigated fight with Russia, has not even noticed.

The Chinese CW forces back out of both America and Russia's networks, destroying all data they could reach as they go. In the aftermath, the Americans and Russians realize what happened, but China left almost no traces of the attacks, and denies all involvement.

A.1.2 Discussion

China has well developed and integrated CNA forces.[32] They have conducted extensive IPB in terms of DOD, Defense Industrial Base, and commercial and public critical infrastructure.[33] China's CNA forces have very likely embedded stealthy attack capabilities in our military and civilian networks via supply chain attacks, have prepared large botnets to use as attack platforms, and have waves of computer viruses prepared to unleash against us.

The supply chain attack mentioned above represents one the gravest risks the US and other technological forces face today. For example, most computing architectures, including those used in weapon and C^2 systems use integrated circuit components and associated software that are developed and produced in untrusted environments. Today's best defensive technology is unable to detect if such devices are compromised, or how they may behave if implanted capabilities are triggered. This is an open research area in cyber security, and is one that needs considerable emphasis from a strategic standpoint.

Conficker, a self-spreading worm in the news recently[34], highlights a pedagogical cyber threat—the armies of compromised networked computers known as botnets. At the time of this writing, the Conficker botnet is estimated at 15 million computers.[35] It is also responsible for crippling military C^2 systems, thus grounding French fighter aircraft. It has also affected British aircraft and naval vessels, including the aircraft carrier Ark Royal.[36] This type of threat is clearly of concern to any modern military.

An enormous amount of damage can be done with botnets. For examples, ask the Estonians[37], or the Georgians[38]. Both countries have suffered crippling cyber attacks in recent years from botnets possibly controlled by Russian sources. Distributed denial of service attacks such as those made possible by botnets are a form of brute force warfare, similar to massing large armies on the field of battle and sending them against a foe. They tend to be very noisy and even though they are detectable, they can be so overwhelming that little can be done about them except to shut off external Internet connectivity to the attacked systems. In fact, this is what was done by Estonia to finally stop the attacks. Unfortunately, that strategy will not work for the US, or even the US military. We are too connected and dependent upon external connections to isolate ourselves and continue to operate effectively.

Botnets can cut both ways. While we usually separate attack and defense capabilities, should we consider using the military networks as botnets? The AF unclassified intranet is comprised of approximately one million PCs, most of which are fairly high-end machines and capable of operating as bots. When tied together with machines across the joint warfighting community the DOD may be able to field a multi-million bot army. Knowledge of this capability may act as a cyber deterrent.

Getting back to the vignette, the scenario is representative of an asymmetric and limited cyber war prosecuted by an adversary hoping to keep our conventional military out of some fight. In preparation of an attack against US interests by a cyber-equipped adversary such as China, we can expect their cyber warfare forces to attempt to achieve the following effects:

1. Distract the populace, government, and military by causing problems at in the US, in our allies' countries, and/or in other theaters of operations. Examples include simultaneous attacks against national critical infrastructure such as financial markets and banking, transportation networks (rail, trucking, shipping), energy production and distribution systems (oil refining and distribution pipelines, power plants and electrical distribution systems), and network-based businesses and information distribution systems (Internet backbones, online business and news organizations). The intended effects would be mass panic and confusion across domestic populace. They may attempt to cause miss-attribution of the attacks to a terrorist group such as Al-Qaeda or a third country such as Iran or Russia with whom the US and allies already have tensions. They may use compromised machines in the US and US and allied military complexes to attack other countries such as Iran or Russia in an attempt to embroil us in a conflict with a third party. They would use non-destructive means and count on this type of cyber attack having short-lived effects, and not causing long-lasting damage which might cause the US and allies to retaliate against their homeland using WMD. Of course, in the case of non-nation states our WMD deterrent will have little effect.
2. Slow down or prevent our deployment of forces to a regional conflict. They would do so by attacking USTRANSCOM and its supporting civilian infrastructure. This type of attack may be more lasting than that against the civilian infrastructure. Equipment may be destroyed and data permanently corrupted.

3. Disrupt our military command, control and communications (C^3) infrastructure. They would accomplish this by using a combination of aforementioned attack capabilities with emphasis on shutting down the network backbones upon which NIPRNet, SIPRNet, and other networks ride. This includes fiber optic links around the CONUS and world as well as jamming or destruction of satellite communications. In theater, they will use electronic warfare extensively. In addition to CNA and anti-space attacks we would expect physical sabotage of this type of infrastructure by sleeper cells or special forces, in CONUS, in theater, and in allied countries. This type of attack may also be more lasting than that against the civilian infrastructure.

As discouraging as it may be, the US and our allies are probably more vulnerable to the type of threat scenario described than any other countries. At a strategic level, we lack an effective means of detecting coordinated attacks across military, governmental, critical infrastructure, and private cyberspace. Nor do we have appropriate mechanisms in place to counter such an attack, or let us operate through it.

What is largely missing from national cyber security discussions is an effective active defense structure: the people, organizations, and partnerships that will pick up where the software, hardware, and policies leave off. This structure must include government (federal, state, and local), law enforcement (federal, state, and local), DOD (active, reserve, and National Guard), the commercial industrial base, and the common use cyber environment. The cyber community needs to be able to develop and leverage intelligence about possible threats to any critical national cyber asset, not just military targets, and to monitor those threats for indications and warning of pending or ongoing attacks. We need to develop the ability to respond, proactively where possible, and reactively where needed, to the full range of cyber attacks. We need to be able to structure our defenses across the entire cyber-dependant community such that we can defend against the threats, and operate through those attacks we cannot prevent.

Just as civilian discussions skirt the issue of including military cyber defense capabilities, many military personnel think of cyber defense as an internal concern. The current DOD cyber defense focus is almost solely on our garrison infrastructure; we act as if that is the most important target and protecting it will ensure our warfighting capability. This perspective downplays our dependencies upon commercial infrastructure such as backbone networks and commercial transportation systems such as those relied upon by USTRANSCOM. From a purely military standpoint, the links between USTRANSCOM and our nation's commerce and transportation infrastructures are absolutely an Achilles Heel. We know how vulnerable these linkages are, are doing very little to protect them, and yet we plan for them to be there when we go to war. We know that our adversaries are aware of all of this, and yet we still do almost nothing. This is not a strategy likely to breed success; in fact, it is not a strategy at all.

Therefore, at a national, strategic level, any discussions of defensive cyber solutions should include the military, and likewise, any cyber defense discussions inside the military should include the non-military communities. We must look past today's traditional patterns of activity, our entrenched "lanes in the road" separating the military, law enforcement, and public and private critical infrastructure, and search for partnerships that will prove effective against tomorrow's cyber threats.

As discussed in Chapter 2, the USAF and DOD are in the process of developing capabilities that will let us exploit and attack the full range of cyber infrastructure upon which our future adversaries depend. This includes the Internet connected systems most people equate with cyberspace, and extends to the SCADA/CS controlling public and private infrastructures, the wired and wireless communication networks, and of course, the warfighting oriented command and control systems.

As we develop these attack capabilities, we should leverage the understandings that grow out of this development to defend our own infrastructure. We cannot effectively attack without understanding defense, nor can we defend without understanding attack. Unfortunately, we tend to separate the two activities and the sets of people performing them, to our own detriment. This vignette and discussion, Two Futures: Part 1, are intended to paint an uncomfortable picture of a realistic threat coupled with our current inability to counter that threat. They represent the state of today's cyber warfare competence. See Section 3.3, Two Futures: Part 2, for how different the outcome may be if the USAF and rest of the US cyber community develop a robust cyber warfare capability.

A.2 Unit-level training

This vignette addresses a current shortfall in cyber training capabilities at the unit level. For the most part, once a communications Airman graduates from technical training they do all of their training and work on operational communications systems. Taking down operational systems for training, whether intentionally or inadvertently due to mistakes, is generally not possible as this would impact ongoing base-wide operations. This restriction severely limits the types of training our communication forces receive. Most importantly, they are not able to practice troubleshooting and error or attack recovery in a contested and degraded cyber environment. Recent advances in computing and communications offer the possibility of creating flexible network simulation environment capable of providing realistic training environments for these Airmen. The emphasis in this section is on training communicators to handle contingencies to supported missions.

A.2.1 Vignette

Airman Jones, a new 1B0X2, Cyber Systems Operator, arrives from technical school to his new assignment in the 245th Cyber Support Squadron. His technical training included the Cyber Fundamentals course all cyber personnel attend, and a technical course in which he learned how to administer servers and data storage systems. As a Cyber Systems Operator, he will be responsible for all the centralized software applications necessary to ensure information is available to support his base's missions. In garrison, this includes the administration of e-mail, domain servers, web servers, and functional software applications. When deployed, he also maintains the software systems used in our Theater Deployable Communication and Air Operation Centers.

He is assigned to a tech control shop responsible for the base network backbone. His initial training consists of familiarization with the base missions and his squadron's responsibilities, and in-depth training on the systems his shop is responsible for maintaining. As his skills develop, he shadows experienced airmen as they perform their duties, and then practices the new duties on training systems. The training systems are flexible tools such as virtualized intranet platform for exercise realism (VIPER)[39] or Simulator Based Training and Exercise Program (SIMTEX)[40], which allow Airman Jones to build up network systems component by component, practice configuration and maintenance tasks, and as his abilities grow, to deal with a wide variety of injected faults and attacks. He sometimes works on skills individually and sometimes as part of a team. The teams consist of personnel from his shop, other parts of his squadron, and sometimes personnel from other units. The flexible nature of the training environment allows for holistic, full-spectrum training under conditions ranging from peacetime to full-up combat in a contested and degraded environment.

When Airman Jones arrives at work his training supervisor, SrA Allen, calls him into the squadron training facility. SrA Allen has configured the VIPER network simulator to emulate the base's NIPRNet infrastructure and tied it into a server rack containing an Exchange email server Airman Jones has been configuring as part of his training. The simulation accurately models the logical network configuration and includes realistic and representative traffic flows throughout the entire network. SrA Allen and Airman Jones discuss the morning's training session, which will center on troubleshooting various problems with the Exchange email services. As the training progresses, SrA Allen inserts various problems into the simulated network, and causes problems with the Exchange server and clients by introducing common configuration mistakes. Airman Jones is able to observe the symptoms each introduces problem causes, and is able to work through his troubleshooting training in tracking down and repairing the root cause of each problem. His actions on the network are captured, which gives SrA Allen a training tool that will help him evaluate Airman Jones' performance by providing a step-by-step record of how he performed in each activity. The accuracy with which the simulator matches the real network makes the training maximally beneficial and is targeted at the specific context of the environment in which Airman Jones will be working. Because the simulated environment realistically matches the actual operational cyber environment, the new Airman has confidence in his ability to help his base operate through an attack. Because his supervisor has seen him work through a variety of scenarios, he also has confidence in the Airman’s ability.

As his training progresses and skills develop, Airman Jones will use the network simulator not only for initial skills training, but also for exercises, and as a laboratory in which new systems, tactics, and procedures can be taught and practiced. Without the simulator training many of these activities would have to take place as either thought exercises, or on the real network, possibly compromising real operations. Other base-level uses of capabilities such as this include using it as a test lab where solutions to problems can be tried in a realistic environment before committing them to the production networks, where hardware and software upgrades can be tried and tested before deployment. It can also be tied to other bases networks or simulators and the national network ranges to provide large scale training and exercise environments.

A.2.2 Discussion

Simulator systems such as that described in the vignette include a combination of real and virtualized computing and network hardware, real and virtual networks, and real and virtualized software applications. The simulations can scale from scale-free Internet sized systems to single machines, and the fidelity of simulation covers the same range. Portions of the simulation can be aggregated into virtual domains with associated aggregated data flows where high fidelity is not needed. For portions of the network needing higher fidelity, virtual machines running real software applications or actual physical machines are used. The data flows can be captured real network traffic, automatically generated using real applications driven by intelligent agents, or a combination of both depending on the needs of the simulation. As users work with the simulation, they connect to and use physical or virtual machines seamlessly.

Simulators such as this are beginning to be available today, and range from complex and expensive to very inexpensive. The AF and other services have been using the SIMTEX, a simulation and training environment to perform crew training and in exercises such as Bulwark Defender.[41] While SIMTEX provides a very high resolution training and exercise capability for network operations center crews, its focus is too narrow to encompass all desired training and exercise activities. VIPER, an initial experiment in designing a flexible and inexpensive network simulator, was explored as a research project at AFIT in 2007.[42] A configuration capable of simulating a base network with the fidelity required to support the training vignette above costs approximately $20,000.00. More work is needed to develop systems such as this, but more importantly, we need to incorporate the capabilities provided by training and exercise laboratories into our overall cyber infrastructure.

We do not expect our pilots to learn to deal with adversary action for the first time in combat--we provide them with a combination of simulator training, local training, and realistic exercises such as Red Flag to develop and perfect their warfighting skills. We need to do the same for our network warriors, no matter their role. The next scenario takes this idea from the individual training level, to base or higher-level contingency exercises in the form of red-teaming.

A.3 Base-level red-teaming

The AF trusts warfighting capabilities that have been thoroughly evaluated through training, exercises, and application in combat. Red teaming is a means of bringing the benefits of exercises such as Red Flag to warfighting units wherever they happen to be located. Participation in Red Flag and related exercises has demonstratably reduced combat casualties and increases warfighting effectiveness. These benefits derive from exposure of combatants to accurate simulations of combat prior to having to engage in actual combat. Likewise, cyber red-teaming exposes the defenders and maintainers of cyber infrastructure to simulated combat situations. This exposure forces the exercising of warfighting skills, helps identify weaknesses and vulnerabilities, and will enhance the performance of these units in actual combat operations.

A.3.1 Vignette

1840 Eastern Standard Time

Its Sunday afternoon, the Super Bowl has been in progress for 40 minutes, and it is shaping up to be a hard hitting game. The cyber defenders and NetOps personnel at AF Base X are glued to their TV's. The rest of the base is very quiet, nearly everyone is off for the big game. Shift change just took place. During handover the outgoing day crews reported only a slightly increased level of scanning activities on the NIPRNet. The swing shift crews raced through their ops checks, finishing just in time for kickoff. The cyber defenses are largely on autopilot; none of the on-duty crews anticipates anything unusual.

The base recently picked up a new flying mission with associated units and cyber infrastructure and data flow needs. As the new units were assimilated into the base operations, the cyber knowledge operators had worked extensively with them to understand the linkages between the mission data requirements and the base cyber infrastructure.

Working together, the local cyber attack forces assigned to an aggressor rotation and the knowledge operators have identified key vulnerabilities in parts of the base cyber infrastructure related to the new units. They also suspect that supporting the new mission areas has led to a decreased defensive emphasis on parts of the existing mission set, and have identified potential vulnerabilities in that area as well. The attack plan specifically targets the identified vulnerabilities. As camouflage, they have prepared a large scale DDOS attack against the base NIPRNet infrastructure. Ideally, the defenders will be able to identify the focused attacks, and will prioritize their efforts appropriately. To aid in this, the aggressors have worked with external agencies and local leadership to ensure the defenders are given appropriate exercise inputs to drive the scenario along the scripted lines as the exercise progresses.

The aggressors have finalized their attack plans, and are preparing to execute. Their goal is to stress the defenders by hitting them simultaneously and in depth across multiple *networks and mission areas. The base Cyber Warfare Group Commander checks one last time with the command post to ensure that no real world operations are pending. All is clear, and he directs the aggressors to strike. They begin by starting up the DDOS from outside the AF network. Several aggressors approach the base, and shake the fence. At the same time three aggressors, a NW officer, a NW NCO, and an EW NCO infiltrate the base by climbing over a fence in an isolated part of the base carrying mountain bikes. Hopping on, they ride quickly into the housing area, and from there head towards the operational part of the base.*

The base security forces see motion alarm activation in several places at the same time. Given the quiet weekend, the NCO in charge decides that it must be a system glitch, runs a quick diagnostic, notes the incident in the log, and goes back to the game.

One of the football teams just scored a touchdown after a long drive--half of the cyber defense troops are cheering, the other half are grumbling. One of the grumblers, a 1B451 Network Warfare SSgt, glances at the situation board and notices that NIPRNet traffic rates inbound to the servers in the base's demilitarized zone are rapidly climbing. He gets his supervisor's attention and points at the board. The supervisor, a 1B073 Cyber Surety MSgt studies the board for a minute, looks back longingly at the game, grabs the remote control and shuts off the TV. Amid a chorus of shouts and groans, she rallies her people around the board and points out the surge in incoming traffic. "Probably nothing important," she tells her troops, "just some ankle biters wanting to keep us from seeing the big game…But still, let's check it out and make sure."

She orders one of her NW operators to check out the overall AF threat board, and another to verify with the base NetOps crew that everything is normal. The local NetOps personnel had also been watching the game, and had not noticed anything amiss. The report back about the overall situation was more interesting. The NW operator reports that he is not able to get access to the threat boards at higher levels in the network hierarchy. She tells him to get on the phone to the integrated network operations and security center (INOSC) supporting their base and find out what is going on.

The aggressor forces have reached the base ops area, and pull uniforms out of their packs and put them on. They quickly set up SATCOM, LMR, RADAR, and cell phone interception and jamming systems. Next, they activate the cell phone jammers, but leave the rest deactivated. As this is occurring, the external aggressors activate a mechanism that continually calls every phone line in the cyber defense and network operations centers.

The defense team is mostly annoyed at the interruption of their game, but some tendrils of alarm are rising in the MSgt's mind. The levels of inbound traffic have reached the point of overwhelming the network links into the base--a situation that should never occur because the higher level network operations and security centers (NOSC) should be throttling the flows to more reasonable levels. The only way this much activity could make it down to a base is if the INOSC itself or the links between the INOSC or the base are compromised. Neither situation boded well for getting back to football. Suddenly every phone in the workcenter is ringing, but nobody is on the other end when one is answered. The MSgt realizes the situation is serious, and tries to call on-call cyber warfare officer to explain the situation, but is not able to get an outgoing line due to the constant incoming calls. She directs one of her troops to step outside the watch center and try to call the CW officer on a cell phone. This does not work either.

The EW NCO climbs up onto the roof of a empty dining hall in the center of the base, sets up and activates a broad spectrum wireless network jammer. This jammer immediately degrades *all base wireless networks. He hops down and heads towards the flightline, where he places and activates another wireless network jammer in the back of a pickup in a parking lot.*

The NW NCO reports that normal phone communications to the INOSC are down--not surprising since they ride the same links that are currently overwhelmed. The MSgt tells him to try the make the call through the backup communications channel which used satellite links instead of fiber land lines. This time he gets through, identifies himself and asks what's going on. The INOSC tells him that it looks like the entire DOD NIPRNet was under attack, and that parts of the attack were originating inside the AF networks.

While the defenders were noticing the overwhelming incoming network traffic and trying to figure out what was happening, the aggressors were working to exploit the vulnerabilities they had identified earlier. In addition to the DDOS, they stealthily infiltrated the base first responder and command network by injecting a network attack into the LMR network used by aircraft maintainers in the new squadrons. Unlike the radio-only LMR networks used by the security police, the new maintainer net is tied into the base network to extend the reach of the handheld radio units. The injected attack quickly finds a vulnerable computer host, and the NW aggressors have their first beachhead in the base network. They quickly work to breakout from that one compromised machine into the core parts of the infrastructure. They are trying to be stealthy, but know they have to work fast, or the local NW defense troops may catch them. They jump from the initial machine into the network backbone, and move quickly from router to router until they are main network control center. One of the attackers quickly accesses the security logging mechanisms, and starts to erase the tracks of their activity from the intrusion detection logs. While she is doing that, another NW connects to the LMR monitoring station, and sets it up to *capture and relay all LMR communications on the base to their console. Soon they are able to hear all security force radio chatter.*

Inside the network ops floor, controlled chaos reigns. The intrusion detection systems are picking up hundreds of potential attacks coming in on the links from the INOSC and alarming non-stop. By now, the NW MSgt has directed one of her troops to go to the command post and inform them of the problem. She gives the on-call CW officer's phone number to the troop using the SATCOM link, and directs him to have the INOSC or anyone else he can talk to get word to the officer that he is needed immediately.

The aggressors are now into the switch controlling the base telephone system. They deactivate the outgoing local network links, forcing all telephone traffic onto the network links to the INOSC. Those links are still completely saturated by incoming attack traffic, thus taking the phones down. They do not have access to the content in the SATCOM links due to encryption, but they do see unusual SATCOM activity beginning. Per the attack plan, they allow SATCOM communications for a few minutes, then jam the local receivers.

At the command post, the duty crew was watching the game, and are surprised by the arrival of the NW airman. They immediately activate their cyber attack procedures. Their outgoing calls do not work any better than the calls made from the NOSC. They respond by calling for a security policeman on the base LMR network to report to the command post.

The aggressors hear the call from the command post.

In the NetOps control center, a cyber surety A1C in the process of training on the base telephone infrastructure notices the switch from the local telephone network links to the INOSC links. He grabs his supervisor and asks what is going on. The supervisor tries to switch the links back, but finds himself locked out of the switching controller. He tries to call the network defense floor, but the internal phones are all still ringing constantly. He sends the airman over with a message about what is happening.

By now, the CW officer (CWO) has made it into the NOSC and is getting briefed by the NW MSgt. They listen to the cyber surety Airman, and dispatch a NW SSgt to the NetOps floor to figure out what is going on over there. The CWO asks if an EW NCO is on duty. There is not one, so he directs that one be called in immediately. Investigating the breadth of the attack, he activates RF spectrum analysis tools, and spots the wireless network and cell phone jamming. Noting that the LMR nets are not jammed, he directs that someone be sent to bring a security forces troop with an LMR to the NOSC. The NW NCO using the SATCOM reports that he has lost contact with the INOSC, probably due to jamming.

He and the MSgt sketch out what they know about what's happening on a whiteboard. Essentially, it is:

1. The links from the I-NOSC are saturated with attacks
2. The I-NOSC reports that the DOD NIPRNet is under attack, and that some of the attack is coming from inside the AF infrastructure.
3. The phones in the NCC are all off hook because that is the only way to stop the constant ringing.
4. Something is going on with the telephone system, with apparent intruder activity in the NetOps control system. Neither incoming nor outgoing calls from anywhere on base are going to work.
5. There appears to be jamming of SATCOM, cell phones, and wireless computer networks, but not LMRs.

6. The command post has been notified, but there is no communications with the command post.

A security force NCO arrives. She reports that there were several seeming anomalous alarms from sensors on the base fences and that the watch officer has directed a search of the base for intruders. Her radio is pressed into use to communicate with the command post. The CWO adds a couple of items to the list of knowns.

7. There may be intruders on base
8. The radio jamming is likely caused by the intruders.

He has an Airman gather the jamming detection and direction finding gear and take it to the front gate to wait for the incoming EW NCO to use. He directs that the EW NCO work with the security forces to locate and neutralize the jammers.

The attackers hear all of the LMR traffic, and decide it is time to start jamming the LMRs--no sense being stealthy anymore. They activate the LMR jammers, shutting down the base LMR network.

The LMR jamming is immediately noticed in the NOSC. At the same time, NW NCOs working to get a handle on the network attack notice unusual activity on the networks associated with the newly installed mission equipment. They report this to the MSgt and CW Capt.

The CW Capt notes that there is so much malicious activity coming in from the INOSCs that his people are unable to make use of the defense detection and prevention systems. He directs that the links to the INOSC be cut off. Immediately, the level of network traffic being monitored drops significantly. He then spawns a virtual copy of the network infrastructure associated with the new mission networks, leaves the incoming traffic from that network connected to the copy, and isolates it from the rest of the network. He has one NW NCO start to analyze and clean up the actual network, and another to monitor the copy for malicious activity. The actions of the intruders are immediately detected in the copied network as they continue to compromise machines.

The CW officer leading the aggressors notices that they have been transferred to a copy network. He tells the attackers to keep prosecuting their attack to provide as much training as possible for the now aware defenders.

Isolating the attackers in the copied network allows the NW SSgt on the NetOps floor to work with the cyber systems operators to regain control of the telephone control switches, and connect them back to the local telephone data lines. The base phone system is now back online and working.

The EW NCO has arrived and the front gate, and was surprised to be met by the security forces with his portable equipment. It takes him all of five minutes to get set up and pinpoint the locations of all the jammers. The security forces take him to each jammer, which he quickly deactivates. He notices that they are all locally owned equipment, and realizes they have all been had by the local cyber attack troops playing aggressor.

By now, the network defenders have completely gained control of the network, and are busily flushing out remnants of the attack activity. All of the vulnerabilities used by the attackers have been identified, and mitigating mechanisms put in place until permanent remedies can be installed. The activity patterns and flows of the attack have been captured, and will be available for training purposes on the base's simulation network.

The EW NCO makes it back to the NOSC with security forces troops in tow. He tells the CW officer what he learned from the jamming equipment. They call the INOSC and tell them the exercise is over, to knock off the traffic generation, and reestablish normal connectivity.

They then go with the security forces troops to the cyber warfare group commander's office in the cyber attack unit's building. They enter to find the commander and rest of the aggressors sitting nonchalantly with their feet up watching the last few minutes of the game. Minor mayhem ensues...

Back in the beginning...

Thurs afternoon before Super Bowl Weekend.

The base cyber operations CC pulls the Capt currently doing an Aggressor rotation, the squadron cyber intelligence officer, and the Knowledge Ops (KO) NCOIC into his office. The base has recently picked up a new flying mission, and they discuss the base's cyber infrastructure progress in integrating the new mission needs and capabilities.

The KO NCOIC expresses concern that his team is struggling to understand all of the new data flows within the new units--they do not yet have a comprehensive understanding of how each flow fits into the mission of the new units. He is also concerned that the NetOps teams may be overfocusing on the "shiny new toys" recently installed by engineering and installation troops in support of the new mission. He's concerned that other parts of the base cyber infrastructure may not be getting the attention it needs. In particular, his troops have heard some grumblings from the security forces about how their radio systems seem to be "breaking up" more than they should. The CC reminds him that the first responder and command nets are made up of land mobile radios tied to the base networks.

The CC directs that an aggressor mission targeting the suspected vulnerabilities is planned for the following Sunday.

A.3.2 Discussion

Overall--I do not want to alienate the bright and capable personnel doing NetOps and network defense today. I would ask that they honestly appraise their ability to counter the adversary action depicted in the vignette.

Emphasis here is on Knowledge Ops, or Mission Assurance. This illustrates the preeminent importance of understanding the warfighting mission of the overall organization. Key to trust of new cyber capabilities in terms of NetOps, Attack/Exploitation, and Defense is the people in the supported missions' confidence their supporting cyber forces understand what they do, how they do it, and what they need to get it done.

In warfighting terms, each mission on a base can be thought of as a center of gravity (COG). Each COG provides some critical capabilities in support of our national objectives. These critical capabilities have critical requirements, which may have critical vulnerabilities. In the case of cyber warfare forces supporting a base level mission, the critical requirements involve data at rest, in movement, or in use. The cyber infrastructure is used to store, move, and manipulate the data needed by the base's organizations. Ensuring its availability when needed requires an understanding of when and how data is used, as well as how adversary action or system failures may impact mission accomplishment.

Our AF is in constant flux, as is how we support the various CCDRs. This necessitates that the cyber leadership, particularly the defense and knowledge operations forces, be integrated into the base/wing mission planning and operations processes.

Red teaming is defined as (emphasis added) : “structured, iterative process executed by trained, educated and practiced team members that provides commanders an independent capability to continuously challenge plans, operations, concepts, organizations and capabilities *in the context of the operational environment and from our partners’ and adversaries’* *perspectives.*"[43] Personnel engaged in cyber red-teaming are adept at analyzing complex cyber infrastructures from different perspectives to identify seams and vulnerabilities across the spectrum of plans, operations, concepts, organizations, and technological capabilities. They bring to the fight an awareness "of the concepts, theories, insights, tools and methodologies of cultural and military anthropology to predict other's perceptions of our strengths and vulnerabilities."[44] They apply critical and creative theorizing and planning in the context of the cyber environment to exploit identified seams and vulnerabilities.[45]

Cyber warfare Red Teams examine the supported organization and missions from the perspective of an adversary with the goal of identifying and exploiting vulnerabilities that allow the compromise or disruption of those organizations and missions. The process of cyber red-teaming benefits the entire organizational structure from the commander on down to the support echelons. The results of red-team exercises provide commanders with awareness of how their missions may be held at risk, improving operational, planning, and OT&E decision processes. The process of defending against red-team attacks affords defensive personnel opportunities to exercise skills and capabilities against a variety of threats. Finally, successful red-team attacks provide insight into cyber vulnerabilities. These insights are critical in adapting and protecting our cyber infrastructure such that we can fly, fight and win in a contested and degraded environment.

Red-teaming is primarily a defensive activity, with the main focus on enhancing our ability to operate through attacks. However, the attack planning and execution processes afford our attack personnel opportunities to exercise their warfighting skills.

Locally assigned red-team personnel will combine insider knowledge of an organization's cyber capabilities and defenses with the attack skills of a unit assigned to understand a particular adversary. For example, a cyber warfare unit assigned to support a war plan for a particular theater will develop a comprehensive understanding of how the cyber warfare forces from adversaries in that theater will operate. They will then use skills based upon that understanding to exercise the defenses of units and organizations likely to be attacked by those potential adversaries.

It is important to note that cyber red-teaming and related exercise capabilities can be used against Federal assets in the Air Force, Joint and Inter-Agency communities. They may also prove useful in combined exercises with state and local governments and civilian critical infrastructure assets. Continuous full-spectrum red-teaming provides many benefits to both the attacked organizations and the attackers. Defenses are continually enhanced, forcing attack skills and capabilities to develop in response.

A.4 CNE by base-level attack personnel

This scenario addresses a new and growing problem in the cyber warfare community: there are too few cyber intelligence-gathering assets. A second problem is that of maintaining currency in cyber attack for our offensive cyber forces. One possible solution takes advantage of the fact that computer network attack is very similar to computer network exploitation, which is an integral part of the intelligence-gathering process. Using cyber attack forces at the unit level in cyber exploitation missions affords them a means of maintaining currency and at the same time satisfies AF and DOD exploitation requirements.

A.4.1 Vignette

Crew turnover complete, two cyber combat teams settle into the team rooms to continue missions still running from day shift. The remaining swing shift crew members of the 312th Cyber Warfare Squadron meet to discuss the evening's missions. Maj Robins, a 17D3 cyber warfare officer and the crew commander, displays the list of taskers the crew needs to accomplish. It will be a fairly low intensity shift, tonight's cyber tasking order (CTO) contains only intelligence needs, it has no active cyber attack missions.

The 312th is an attack, defense and exploitation unit that specializes in power generation and distribution systems. See Section 2.4 for a list of cyber network classes in which a unit such as this might specialize. For the last several weeks they have primarily been working intelligence taskings in support of intelligence preparation of the cyber battlespace of Country X as part of a geographic CCDR’s contingency planning process. The various combat teams have been working their way throughout X's power generation and distribution systems, mapping the networks, identifying vulnerabilities, and implanting exploitation and attack capabilities. The cyber intelligence gathered is combined with other forms of intelligence to enhance the CCDR's understanding of a possible battlespace. Ultimately, should the US and Allies go to war with Country X, the work done by the 312th will enable the synergistic employment of cyber capabilities in and through the adversary's network with kinetic capabilities to deny or degrade that adversary's warfighting capability.

One of the tasks is to explore the linkage between the power grid and a ballistic missile factory. Maj Robins assigns that task to the cyber combat team headed by Capt Jones, another 17D. He directs Capt Jones to coordinate with the team working the exploitation of the SCADA/CS infrastructure of that factory. The CTO allocates those missions to the 111th CWS, a National Guard unit which specializes in aerospace industrial manufacturing systems. Capt Jones looks through the mission rules of engagement and tells Maj Robins that she will also maintain a link with the signals intelligence organization responsible for that region to maintain. Intelligence reports hint at increased activity in that factory, and it is imperative that any adversary awareness of the 312th or 111th activities be detected as soon as possible. The team led by Capt Jones consists of TSgt Andrews, a 1N4 cyber intelligence analyst with 10 years experience in power systems, SSgt Nobles and SSgt Rich, both 1B451 Network Warfare Operators, TSgt Lacey, a 1B178 Control Systems Operator, and SrA Thomas, a 1B054 Computer Programmer. Their interface in the 111th is Maj O'Brian, the Guard 17D3 team lead. The 312th and 111th are not strangers, they work extensively with each other on taskers like tonight’s, but have also partnered in national-level defensive exercises and a handful of operational missions.

The team gathers in a team room for a briefing by TSgt Lacey about what is known about the systems they will be working, and about their goals for this shift. They work together to plan their tactical strategy, check out the appropriate attack and exploitation weapons from the armory, and connect to the access infrastructure attached to the adversary networks. Previous teams had mapped out the higher logical levels of this part of the network, the first tasks tonight involved ensuring that earlier intelligence was still valid. The initial exploration of the network validates the previous results, and the team settles into the tasks on the CTO.

In another theater, SIGINT sources detect that an adversary in Country Y has ordered the startup of chemical factory currently under a United Nations Security Council closure order. The geographic CCDR for that theater already has authorization to use force in preventing factory startup. He turns to his planning staff and asks what his options are for dealing with the situation. The contingency plans for that country are opened, and his staff notes that the factory can be safely destroyed using cruise missiles, less safely by sending in stealth bombers (the US does not currently have air superiority over Country Y), or safely by disabling it using cyber attack. The CCDR calls CCDR USSTRATCOM and asks if the cyber operation can be executed quickly.

CCDR USSTRATCOM's staff opens the contingency plans, and notes that the factory can be disabled using SCADA/CS attacks. They check the CTO for the night and discover that the 312th is performing cyber exploitation missions on an equivalent SCADA/CS that night. A text message through the cyber C^2 system verifies that the 312th is capable of taking down the problem factory within 30 minutes or less using preplanned capabilities. The USSTRATCOM staff passes this option back the geographic CCDR. He issues the order to take down the factory.

Back at the 312th, the contact from USSTRATCOM served as a warning order, and the exploitation team set up the required equipment and weapons to take down the factory. They turn the current exploitation mission over the 111th for an hour. When the attack order arrives, they execute the preplanned options. Within just a few minutes the power switching center at the Country Y factory experiences a carefully planned sequence of upset events, leading to a cascading failure that destroys critical power system components. The factory is down, and will not be coming back online for at least several weeks. Notification of success is passed back up the chain and the attack team settles back into exploitation mode.

A.4.2 Discussion

In one model for organizing cyber warfare forces, each base has some level of attack and defense cyber forces. Some bases will have multiple squadrons organized in cyber warfare groups tailored to support combatant command requirements for capabilities in specific network classes. Others will have a blended squadron with both attack and defense capabilities. All cyber warfare units will have basic proficiency in IP network attack and defense. At a minimum, the skill makeup and mission capability sets for a squadron or group will be tailored to support the missions on their assigned base. Specialized capabilities against particular technical or functional network classes may differ enough from basic IP networking in terms of technical differences and/or scale of required support to the CCDRs to require units which specialize in those mission areas. Examples are provided in Section 2.4.

In general, computer network attack and computer network exploitation are very similar activities at the tactical level of operations. Traversing a network to implant an exploitation capability requires essentially the same capabilities and skills as traversing the same network to implant an attack capability or achieve some specific warfighting effect in cyberspace. There are certainly differences between the two missions; Typically, CNE for espionage purposes needs to be stealthy, may operate undetected for extended periods of time, and may require covert channels back out the exploiting organizations to exfiltrate data. Disrupting system behavior is usually undesirable from an exploitation perspective. Depending on the mission context, CNA may be stealthy or noisy. Disrupting system behavior in some way is usually the goal of network attack, and there may not be any requirement to exfiltrate information from targeted systems.

While the techniques used in CNE and CNA differ little, if both types of operations are taking place in a shared region of cyberspace they must be coordinated and deconflicted carefully. The tension between these two types of missions causes significant concern in today's developing cyber warfare environment. We have different organizations performing CNE and CNA, and are actively exploring how to deconflict the two types of missions. One way to ease CNE/CNA situational awareness and deconfliction concerns is to have the same units performing both missions. A second concern is that we do not have enough CNE or CNA capabilities in terms of both scale and scope of network classes. Developing units that specialize in specific network classes is an expensive proposition. Developing separate exploitation and attack units for a particular network class is likely to be even more expensive, thus providing more incentive to keep both capabilities in the same units. Finally, attack skills are expensive to develop and have short shelf lives--maintaining currency for a force large enough to support large-scale future combat situations will be a major challenge. Having those forces perform CNE missions on a day-to-day basis will allow them to keep their attack skills current.

Having service forces performing CNE would not necessarily conflict with the current intelligence community's CNE. A model in which service units provide CNE capabilities to combatant commanders and other entities such as the intelligence community could help satisfy both national-level intelligence needs and CCDR contingency and crisis planning needs.

A.5 Integrated Operations

For many Airmen, cyber warfare operations seen distinct from traditional kinetic operations. This vignette illustrates how well developed and integrated cyber operations both support and are supported by land-based and airborne operations.

A.5.1 Vignette

A US bomber performing an interdiction mission behind enemy lines drops conventional bombs on targets such as bridges and fuel depots, but also drops a number of specialized munitions containing cyber warfare payloads into a region where adversary reserves are forming up. When they hit the ground these cyber weapons stealthily activate and begin sniffing the radio frequency (RF) spectrum in search of a particular type of emission. The target RF activity belongs to the adversary tactical data links used to coordinate activity between land forces.

A CWO Capt directing penetration of the TADIL connects to the dropped cyber weapons and begins attack operations. His team rapidly compromises the enemy TADIL, and the Captain reports success and begins planned intelligence exploitation operations. Shortly afterward, the satellite communications supporting a special operations force (SOF) team hidden in the enemy’s reserve region takes active jamming from the enemy. This leaves the SOF team without communications capability. Notification of the lost connectivity is passed up to the Joint Task

Force current operations planning team. The CWO Maj on that team determines that the adversary TADILs just compromised can be used to provide communications for the SOF team. He directs the Capt to enable SOF C2 through the use of the compromised TDL network. The JFC now has insight into the enemy activity through the exploitation of the TDL, and also an unanticipated emergency C2 capability for portions of his own forces.

As operations continue, the in-theater CW forces work to locate the sources of satellite jamming. The CW ops major works with his kinetic collegues and determines the jamming sources are in the kill box for an air strike, and that an air strike is the best way to negate the enemy actions. The JFC orders the strike. Within a few minutes the coordinates are passed to a loitering B52 which drops anti-radiation munitions (ARMs) on the targets. The ARMs home in on the RF emissions of the jammers and hit them. We see the satellite links come back up and then go back down. At the same time we capture enemy chatter over the compromised TADILs about a near miss at one of the jamming locations. The B52 is retasked to strike that jamming location with larger precision munitions based upon the captured battle damage assessment. This time the jammers do not come back on line and normal SATCOM links are reestablished with the SOF forces.

A.5.2 Discussion

At the 30 thousand foot level, in a combat scenario such as this, all DOD forces involved are fighting in support of the joint force commander (JFC) responsible for operations in a particular campaign or theater. The JFC has a battle plan that articulates the overall military desired end state, the main objectives which will result in that end state, and the offensive and defensive effects needed to achieve those objectives. These objectives are then tied to centers of gravity, which represent sources of warfighting power. A COG provides some capability important to the war effort, the generation of this capability requires resources, and may have vulnerabilities. Adversarial COG vulnerabilities are what we target with our offensive combat power. Our defensive capabilities are used to protect our own COG vulnerabilities. Another part of an operational plan is the commander's critical intelligence requirements (CCIRs). These are the specific intelligence data the JFC needs about the status of combat operations in order to make good decisions. For more information about the joint operations planning process, see Joint Publication 5-0.[46]

In our scenario, the CWO Captain was initially tasked with gathering intelligence information in support of a CCIR. In this case, gaining access to the targeted data required that the cyber warfare team successfully penetrate an adversary's battlefield data network; the US term for such networks is tactical data links. While TADILs may be connected to outside networks such as the Internet, in general they are not, tending to be local to a set of ground, naval, and/or aerospace forces. Networks such as TADILs are good examples of mechanisms by which US, allied, and adversarial forces operate and perform command and control functions at the tactical level. They differ significantly from country to country, and may or may not be interoperable between different components of a military force. For example, not all US TADILs used by land forces can be used to communicate with aerospace or naval forces. The ability of such networks to operate in a contested, degraded environment varies as well, from simple radio links to encrypted systems incorporating anti-jam capability and other protective measures. In general, penetrating such a network requires very specialized skills, weapons, and access to the region in cyberspace in which the network operates. This access may require the CW forces to be in theater, or it may be possible to place some sort of local access mechanism in theater and connect through a reach-back architecture to CW forces located behind the lines or back in the CONUS. The access mechanism may be airborne, in space, or on the ground or sea.

The scenario above made use of a notional local access and reach-back mechanism. Weapons that help gain access to non-Internet connected systems such as this will be important components in the arsenal of our future cyber warfare forces. Much of our current cyber warfare focus is upon the unclassified and classified IP networks used to connect desktop and laptop computers together. These interconnected systems do indeed provide critical capabilities for us and our adversaries, but they represent just a small part of cyberspace. Other non-IP networks range from TADILs and other closed battlefield networks to land mobile radio (LMR) nets to the SCADA/CS networks used in manufacturing, distribution and critical infrastructure control. Supporting the full range of effects needed by JFCs in the future necessitates developing capabilities that operate in or through the full spectrum of the networks making up cyberspace.

Another technology mentioned is the anti-radiation munitions. ARMs with increasing levels of capabilities have been in the DOD inventory for decades. Early ARMs were used solely to suppress enemy air defense systems; however, newer weapons of this will need the capability to target a wide range of emitters such as the jammers used in the scenario. As modern militaries such as ours make more use of RF networking, cyber warfare forces will develop mechanisms to jam those networks. Just as we are developing small, simple, inexpensive UASs for ISR

A.6 Two Futures: Part 2—Tomorrow

The conflict in Part 1—Today did not go so well for the US or our allies, in part because we were not ready to handle the type of cyber warfare even a modestly competent adversary could throw at us. Some of the problem had to do with internal military defense needs, some was a lack of appropriate intelligence capabilities, but a lot had to do with the lack of partnerships between military, government, and private cyber infrastructure and defense capabilities. The vignettes and associated discussion contained in this appendix present a partial vision for how we may organize, train, and equip our cyber forces in the near future. The vignette below takes advantage of the envisioned capabilities, and results in a different outcome to the same type of attack.

A.6.1 Vignette

Starting as much as years prior to the confrontation, US military and law enforcement intelligence capabilities monitor the construction of Chinese botnets across the world. In particular, the botnets in the US and Russia are noted, and mechanisms are put in place to co-opt them for friendly use if needed. All Chinese owned botnets are monitored for I&W.

Knowing that supply chain attacks are so difficult to detect, the US military engineers its C^2 systems to be robust in the face of attacks or failures from within. The defenses against such attacks have both technical and human components. The forces using and actively protecting these systems regularly exercise operating under degraded conditions in which parts of their weapon systems may be compromised. They are able to react quickly and correctly when an attack or other problem occurs.

Over the last few years, the US military has developed a full-spectrum cyber warfare capability. These forces and capabilities include Title 10 active duty/reserve and Title 32 National Guard units. The National Guard cyber units in each state have robust connections with the state and local law enforcement and commercial cyber infrastructures. Regular red teaming occurs at all levels of the cyber infrastructure. Likewise, the defensive relationships and protective measures are also regularly exercised across the spectrum, from natural disasters to unlimited cyber war against the US. When DHS has a need for defensive cyber support, DOD, law enforcement, and commercial industry can answer the call.

Now, back at the beginning of the scenario, US and Russian naval forces are operating near each other in the Gulf of Aden off of Somalia on anti-piracy missions. Using a supply chain attack, Chinese cyber warfare forces have compromised the fire control systems on both an American destroyer and a Russian frigate, and have the ability to aim and fire them at will as soon as the weapons are placed on alert status. The Chinese PLA has placed a device that emits radioactivity simulating a small nuclear weapon on a Liberian freighter, and arranged for its capture by Somali pirates. Chinese Special Forces in Pakistan and Kenya near suspected al Qaeda locations engage in a lightly encrypted and highly charged satellite phone exchange about the "hijacked Fist of God." Both American and Russian SIGINT operations pick up the transmissions and rapidly decode them. The two militaries employ sensors capable of detecting the presence of the suspected bomb, and quickly identify the hijacked vessel as containing a suspected nuclear weapon. Both the Russian and America task groups dash toward the ship.

At the same time, Chinese CW forces have completed their preparations for a massive and sustained attack against America's critical infrastructure. Their extensive infiltration of DOD's networks over many years has yielded immense amounts of information about how the DOD operates. They used this information to highlight vulnerabilities, and crafted and implanted stealthy attack implants in crucial nodes of the DOD's warfighting command and control networks.

As the battle groups converge in the Gulf of Aden, China's cyber warfare forces prepare two large botnets for action against targets in the US and Russia. The first botnet was constructed primarily under contract by Russian organized crime organizations. Carefully selected information about parts of the botnet were leaked to the US intelligence sources in a MILDEC campaign, with the intent of leading the US to believe that the botnet was under Russian military control. Likewise, the Chinese leaked the existence of the second botnet to the Russian's by planting information about it that leads back to the US military.

The US military intelligence community sees the botnet activity, and because of its timing compared to the building crisis in the Gulf of Aden, raises a concern to the highest levels of our government, and raise military alertness. The linkages between the Chinese botnet in Russia and the Chinese botnet in the US are also noted. Senior civilian decision makers authorize the release of I&W to Russia, and both sides slow down activities off the coast of Somalia.

China's CW forces selectively engage the first botnet in DDOS attacks against key parts of the USA's economic and transformation infrastructure. The DHS works through the carefully exercised defense procedures and halt the attacks before they get underway. A combination of law enforcement and National Guard capabilities active the co-opting mechanisms, and lock out the Chinese CW command and control. At the same time, the Chinese activities across the Internet are carefully monitored and sufficient evidence is captured to prove without a doubt the intent and involvement of the Chinese government. This information is passed to news organizations in the US, Russia, and China. This part of the attack has been countered.

Because the US and Russians have slowed way down and are containing the hijacked ship from a distance, the Chinese electronic warfare forces cannot effectively jam their radio communication. Their jamming is detected, and is readily countered. Concerned that the Chinese vessels doing the jamming may have other hostile intent, both the US and Russians train their weapons on them. The Chinese naval commander detects this act, and instead of firing the US weapons at the Russians, he chooses to exit the region at top speed. This aspect of the attack was also a failure.

Given the repeated covert warlike acts by Chinese forces, it is now apparent that they are trying to entangle the US and Russia in a conflict. Why they might wish to do so is quickly discovered when intelligence assets focus more attention on Taiwan. Sufficient warning is given to the Taiwanese government that they are able to protect themselves against the Chinese SOF attack. The US and Russia very quickly move naval assets into the Straights of Taiwan, effectively preventing the Chinese attack from occurring.

At this point, the Chinese give up, and our investment in robust cyber warfare capabilities has prevented a tremendous crisis. The US and Russia broadcast to the world what happened, and future acts such as this are forestalled.

A.6.2 Discussion

The cyber research and development community has known for many years that no information system will ever be invulnerable to attack. Therefore, the emphasis for security must concentrate on engineering systems capable of operating correctly through attacks. We must exercise operating in contested and degraded environments such as those we are likely to face in real world situations. Our focus must cover the entire interdependent cyber infrastructure, not just military or civilian stovepipes. Capabilities such as red-teams, active defense forces, and well thought out and supported connections between the various aspects of our cyber infrastructure will enhance technological improvements in dramatically improving our overall cyber security.

Appendix B – Cyber ACTS/SAASS Continued

At the dawn of Airpower, the Army Air Corps created the Air Corps Tactical School—a school focused upon developing tactics, techniques, procedures, and doctrine about how to best use airpower in war. Currently, the Air Force School for Advanced Air and Space Studies grows highly capable warfare strategists in support of the joint fight. We need to blend ideas from these two programs into a school which grows cyber power leaders capable of guiding the AF into a future in which we can fly, fight and win in air, space, and cyberspace in support of America's military objectives.

B.1 Problem Statement and Introduction

The Air Force is struggling with how best to develop offensive and defensive cyber warfare capabilities. Our vaunted warfighting prowess across the land, sea, air, and space domains relies upon our ability to maneuver freely within cyberspace. Preserving that ability is a critical defensive requirement. We must also develop the ability to hold at risk our adversaries' ability to maneuver within cyberspace. This chapter introduces a concept for how and why the Air Force should develop cyber-oriented warrior-scholars capable of shaping the Air Force fight in cyberspace. This concept is substantiated by discussing how we develop advanced strategists and airpower advocates, describes an existing Air Force graduate education program which largely fits the bill, explores potential downsides, describes how this proposal fits into the ongoing cyber warfare force development effort, and finishes with courses of action and a recommendation.

In many ways, cyber warfare is in its "Billy Mitchell" days, analogous to the advent of airpower prior to World War II. We are aware of potential and actual risks in this new domain but do not fully understand them. Just as the Air Corp Tactical School was the birthplace of modern airpower, we need a school which develops cyber-oriented warrior-scholars who can help guide the US Air Force through its transformation into a force capable of flying, fighting and winning…in air space, and cyberspace. One possible means to develop such leaders is to add a second year of technical study of the cyber domain to the operational art and science foundation provided by Air Command and Staff College. The second year Cyber School already exists within Air University; it is the Intermediate Developmental Education Cyber Warfare program at the Air Force Institute of Technology.[47] I propose the USAF create a two-year professional military education path consisting of ACSC followed by AFIT's Cyber Warfare program, to parallel the current path of ACSC followed by the School of Advanced Air and Space Studies.

This article expresses concerns and proposes a partial solution to the AF community about a strategic question: how do we develop the leaders who will in turn shape the cyber fight of the future?

B.2 So, what's missing?

China, North Korea, and other countries have well-developed graduate education programs in cyber warfare.[48,49] Additionally, these nations send students to America's finest graduate institutions for master's and doctoral degrees in cyber disciplines such as computer science, computer engineering, and electrical engineering. These students go back to their countries and apply their new knowledge towards developing cyber warfare capabilities. While those countries may or may not use those capabilities against us, the model those countries are using is one we need to consider. To understand why, consider as a starting point the distinction between education and training. Air Force Doctrine Document 1-1, *Leadership and Force Development*, describes the difference as follows,

> Education provides critical thinking skills, encouraging exploration into unknown areas and creative problem solving. Its greatest benefit comes in unknown situations or new challenges. Thus, education prepares the individual for unpredictable scenarios. Conversely, training is focused on a structured skill set, and the results of training performance should be consistent. Thus, training provides the individual with skill expertise. Education and training together provide the tools for developing Airmen.[50]

The current Air Force and DOD methodology for developing cyber warfare forces, including the future leaders in this domain, is heavily focused on training instead of education. Even training is expensive, therefore in a budget-constrained training environment we are essentially fielding forces that are trained and equipped to respond to a limited range of scenarios. These forces are largely out of their depth when faced with the unpredictability that a trained *and educated* adversary may be able to impose upon them. This is not a winning strategy—in fact, it is not a strategy at all! While we build cyber capabilities, we need to be able to counter their “best athletes” with our own “best athletes,” led by highly educated and innovative warrior-scholars.

Fundamentally, operations in a new warfighting domain such as cyberspace take place in a fog of uncertainty, full of unknowns and new challenges. The situation we face today is highly analogous to that faced by early Airpower advocates during the interwar period. A comprehensive understanding of cyber warfare does not exist, there are a handful of outspoken cyber warfare proponents, and most people in the AF and other services have very little idea what exactly cyber warfare brings to their own mission, much less the joint warfighting environment. In many minds, cyber warfare is synonymous with communications, cyber attack means corrupting web pages, and cyber defense means keeping our web pages safe from attack and removing viruses from our administrative networks. From this perspective, it is hard to see how cyber warfare has much to offer as a warfighting discipline, and therefore there is little popular support for the AF’s push into cyberspace.

The popular perception is not far off mark. Cyber warfare capabilities in the AF and DOD are still nascent, and many of the capabilities we do have are classified to the point that joint force commander planning staffs cannot readily incorporate them in plans. This leads to a two-fold chicken-versus-egg problem. Inside the AF, it is difficult to develop advocacy for as yet undeveloped and unproven cyber capabilities, forces, and organizations, given that supporting cyber capability development means not supporting some other proven capability. Externally, because we do not yet have much to offer the joint force commander in terms of trustable, usable cyber warfighting capability, it is difficult for the JFC to articulate requirements for capabilities the services can then provide, much less plan for their use in combat.

How do we address these problems? We start with an understanding of the effects needed by the JFC in current and near future conflicts, and the capabilities provided by existing kinetic warfighting capabilities. This is knowledge that many “operators”, or warfighters, in today’s AF possess, but which is not as well understood by the developing cyber warfare force and supporting science and engineering community. Equally important is awareness of today’s cyber warfare technological capabilities, and where cyber capability development has the potential to go in the near future. This knowledge is primarily possessed by a handful of scientists and engineers. A leadership-oriented education program combining both sets of understanding and focusing on creative thinking and problem solving will produce highly innovative, technically competent warfighters. These officers will be able to lead the fight, identify needed improvements or new effects, and work with the research and development communities to produce new warfighting capabilities.

This needed innovation is not the sole responsibility of the warfighter. It requires the involvement of the research, technology development, planning, and programming communities, and others. However, what has been largely missing to date are active involvement of operators in the technology development process and openness to innovation. As a service, we have been in similar situations before. Perhaps the best analogies come from the dawn of airpower, when technically oriented senior leaders shaped the future AF through their struggles to provide solutions to warfighting problems.

B.3 Historical Analogues

Historical analogues can be found in the struggles of leaders such as Lt General “Pete” Quesada[51] and General George Kenney[52] as they tackled the integration of airpower capabilities into the US arsenal before, during and after WWII. Both Quesada and Kenney commanded American forces at the dawn of airpower, in the context of a world war, and were virtually awash in a sea of change. The manner in which these two iconic leaders dealt with our nation’s warfighting problems, both with regards to their innovate exploration and adoption of technology, and their pragmatic approach to warfighting, offers valuable insights to the AF as we learn to fly, fight and win in cyberspace. Quesada and Kenney both dealt with strategic and tactical puzzles by tossing aside dogma and searching for ways to improve the warfighting effectiveness of their forces. These searches focused on continuous improvement, and were characterized by extensive experimentation followed by the adoption of workable ideas.

What is particularly interesting about all of this innovation is that the exploration proceeded during the heat of battle. This idea is anathema in the AF’s current risk-averse culture. Both Quesada and Kenney had a complicated relationship with the prevalent service culture of their day which emphasized the importance of strategic bombing over close air support and interdiction. A similar situation exists today in the AF's understandable focus on use of the air weapon over cyber or space weapons. Both leaders had backgrounds which proved useful in growing as commanders in such a dynamic and difficult period. Their Army background and educations gave them a shared language with the ground commanders they supported. As junior officers, they both spent time with senior leaders of their service, and gained broad insights into many of the important issues of the period. Upon taking command, both emphasized frequent meetings with the ground commanders to enhance the situational awareness of both sides. Both Quesada and Kenney spent a great deal of time in the field, identifying problems, devising fixes, recognizing accomplishments of their troops, and in general, leading from the front of efficient, energetic, and effective organizations which thrived in a wartime environment of change.

From a cyber perspective, we need to grow leaders who will likewise lead from the front while seamlessly integrating cyber warfare into the overall warfighting effort. Such leaders will need to work closely with the leadership as well as rank and file of the organizations that rely upon the infrastructure for which they are responsible. In ways, this is analogous to the support Quesada and Kenney provided the ground commanders.

In particular, the foundation of modern society and our military effectiveness is information-based and is vulnerable to cyber attack. Warfare theorists such as Martin van Crevald inform us that technology throughout history has brought promise of increased warfighting power, but is also characterized by vulnerabilities and limitations. Victory in future conflicts depends upon understanding and overcoming the limitations of technology, while minimizing dependence upon vulnerable technology.[53] Since it seems unlikely that we will somehow divest ourselves of high-tech, information-dependant gadgets, we need to figure out how to fly, fight, and win in the face of determined and capable adversarial actions against those information systems. This will require innovation, courage, and conviction on the part of our leaders. The risk-taking and mission-oriented focus of Quesada and Kenney offer inspiration and motivation in how they managed the interplay of command and technology in the context of war.

In summary, new capabilities will require leaders with the flexibility to develop new TTPs and doctrine in conjunction with research, technology developers, and operators. To produce leaders like this requires a mix of education that provides broad understanding of theory and provides problem-solving skills, training in a variety of weapon systems, operational experience, and a solid understanding of how the joint fight takes place. Creativity and problem solving skills will be important characteristics of the future cyber warrior, whether they are planners on a JFC staff, researchers, operators in the field, or on a staff. The cyber schoolhouses must become laboratories in which cyber warfighting capabilities can be conceptualized and developed much as the Air Corp Tactical School was for Quesada and Kenney prior to WW-II.

B.4 What is the value in a second year school?

Air University's SAASS is the USAF's second year graduate school focused on developing strategists and warrior-scholars who possess superior abilities to develop, evaluate, and employ airpower in conjunction with land and sea capabilities in complex warfighting environments.[54] Its predecessor, the School for Advanced Airpower Studies was created in 1988 primarily to develop strategists.[55] The Air Force re-designated SAAS as SAASS in 2002.

The Army's School of Advanced Military Studies, the Naval Operational Planners Course, and the Marine Corps' School of Advanced Warfighting are equivalent programs intended to develop advanced warfighters in their respective services.[56] The Joint Advanced Warfighting School focuses on developing advanced campaign planners and strategists for the Joint Staff and combatant commands.[57] All three service schools build upon an operationally-focused foundation provided by first year graduate studies in the Air Force's Air Command and Staff College, the Army's Command and General Staff College, and the Marine Corps' Command and Staff College residence programs.

Graduates from all four advanced service schools have been some of the most influential strategists and leaders in their domains. They are able to leverage a broad understanding of the art of war and the dynamically evolving capabilities of our military forces into strategies that prove effective against our enemies. The model of enhancing the broad warfighting backgrounds provided to in-residence IDE graduates with advanced education in a particular area is very attractive in terms of growing influential and effective leaders who possess both depth in their warfighting domains and breadth in terms of how to support the joint force commander in achieving operational and strategic objectives.

B.5 Why not just add more cyber to the SAASS curriculum?

When thinking of where to add advanced cyber education into the overall AF education system it is logical to consider enhancing an existing advanced program such as SAASS. Simply put, however, SAASS is not the right place in which to develop a cyber parallel to ACTS. While SAASS was originally intended to be an airpower school, its charter to produce advanced warfare strategists drove a curriculum that is largely service agnostic—its graduates are able to develop joint strategies that are then realized using the full spectrum of warfighting capabilities across the air, land, sea, space and cyberspace domains. [58] SAASS students extensively examine theory and historical experience and develop an enhanced ability to think critically about how best to apply modern land, sea, space, cyberspace, and air power across the entire spectrum of conflict.[59] The curriculum and focus are general purpose, and non-technical.

In contrast, cyber warfare is inherently highly technical, and is new enough that the leaders in this domain must likewise be technically proficient, much as Quesada and Kenney's technical depth enhanced their successes in terms of early airpower development. Adding an appropriate level of theoretical and engineering depth to SAASS would not only be very expensive in terms of hiring appropriate faculty, but would likely severely shortchange the strategy components of the curriculum. The bottom line is that cyber warfare TTP, doctrine, and capability development do not reasonably fit into a curriculum focused on the study of domain agnostic strategy. This dilemma drives the need for a separate school.

B.6 Hasn't this been proposed before for space?

The AF space community faced an analogous situation in the 1990s, and advanced similar ideas about the need for space power advocates. The AF decided to include material about space in the SAASS curriculum and to keep air and space officers together in the same program.[60] The goal of having air, space, and cyber power advocates and strategists in the same room makes a great deal of sense, and of all the AF PME schools with the exception of AFIT, SAASS has incorporated the most cyber material into its curriculum. At this point, the analogy breaks down. Instead of focusing on general strategy, we need a program focused on understanding the technology and theoretical underpinnings of cyber warfare capabilities and which seeks to understand how those can be leveraged alongside the rest of the joint capabilities in meeting JFC objectives. In this, the argument for a separate school parallels the need for Air Corps Tactical School before World War II. The current cyber strategists are trying to lift themselves up by their bootstraps and programs such as AFIT's cyber warfare degree can help significantly.

B.7 What is AFIT's IDE Cyber Warfare Program?

AFIT developed the IDE Cyber Warfare program to support the handful of IDE students sent to AFIT in lieu of the in-residence ACSC program. The first students entered the program in 2007 and graduated in 2008. Because of its origins as an IDE program, the one-year ICW program is already matched up with SAASS starting and graduation dates, and culminates in a Master of Cyber Warfare degree.

ICW develops technical and leadership proficiency in both CW and CO, with emphasis on the operational and strategic levels of war. The curriculum emphasizes education and research into both offensive and defensive CW operations. Ultimately, it develops cyber warfare proponents who understand and can articulate how best to apply cyber power in achieving military objectives. While ICW is cyber-focused, the curriculum's foundations include the full spectrum of IO as defined by joint doctrine. ICW's program of study includes a wide variety of disciplines, including both technical and nontechnical aspects, of the topics below.[61]

- Influence operations, psychological operations, and deception
- Command and control warfare
- Electronic warfare
- Electronic sensors
- Communications systems and networks
- Computer and network attack, defense, and exploitation
- Threat / vulnerability assessments and risk management
- Legal / ethical aspects of cyber warfare
- Strategic and tactical planning for cyber operations and warfare

Cyberspace as a warfighting domain is undergoing rapid transformation, a trend that will continue for the foreseeable future. This implies that the educational development of our cyber leaders will require correspondingly rapid transformation. ICW's curriculum is developed and taught by the faculty of the AFIT Center for Cyberspace Research (CCR), which the secretary of the air force (SECAF) and chief of staff of the Air Force (CSAF) recently designated as the Air Force's Cyberspace Technical Center of Excellence.[62] In this role, CCR is a unifying body for promoting cyberspace education, training, research, and technology development. Its location at the juncture between the operational USAF cyber forces and various cyber research, education, and training communities across the Air Force, the DOD, and national organizations ensures that programs such as ICW stay on the cutting edge of technology and theory.

B.8 Side issue—Cyber Ph.D.?

SAASS is working through Congress for permission to add a Ph.D. follow-on track for a handful of SAASS graduates. AFIT is already a Ph.D. granting component of Air University, so the possibility of a Cyber Ph.D. in the future is readily obtainable should that make sense for the Air Force. The USAF is debating the need for doctoral-level warrior-scholars who are also senior officers. One commentator summarizes the problem as follows:

> The Air Force has too few senior officers who are bona-fide warrior scholars; as an institution we have failed to promote warrior-scholars to the senior ranks; we have failed to do so for a number of reasons, including the difficulty such officers face in achieving the competing demands to become both a warrior and a scholar, the possible reluctance of senior officers to promote those unlike themselves, and the lack of incentives (or personal motivation?) for officers who have achieved scholar status to also attain "warrior" status and thereby to achieve senior officer rank.[63]

The Air Force primarily develops Ph.D. level warrior-scholars to serve in academic and research roles. Between the time required to earn the degree and the time in academia or research laboratories required to pay back the degree, our officers have missed many of the warrior-leader opportunities afforded their peers. In general, this makes them less competitive for promotion to senior leadership. Cyber power, in particular, may benefit from having senior officers who not only have warrior credentials in terms of operational and command experience, but also the innovative and advocacy abilities afforded them by the scholarly work that led to a doctoral degree. An AFIT cyber Ph.D. along the lines of the proposed SAASS airpower Ph.D. degree would focus on developing lieutenant colonels and colonels to become senior warfighters and leaders in the cyberspace domain rather than just serve in academic or research roles.

B.9 Whom and how many should the USAF send to ICW after ACSC?

Following the model of SAASS, a centralized process should competitively select officers from a pool of volunteers. While all first-year residence school graduates should be eligible, the main goal of this program is to develop cyber-power advocates who will lead the cyber warfare forces in developing cyber capabilities in support of JFC objectives. Thus, emphasis should be on officers who will likely lead cyber units, integrate cyber into the planning process, or act as cyber advocates on joint and service staffs. Air Force Specialty Code 33S communications, 14N intelligence, 11X pilots, 13S space and missile operations, and 12X electronic warfare/navigator officers and their sister service peers would be the most likely prospects for attending such a program.[64]

How many cyber warrior-scholars do the Air Force and DOD need? SAASS graduates 40 advanced strategists and airpower advocates each year. Forty cyber graduates annually would be a terrific start. However, an initial cadre of 15 to 20 cyber-oriented warrior-scholars, able to bring to the fight both the operational breadth provided by the in-residence IDE and the technological depth provided by ICW, will be a powerful force for development of cyber capabilities in support of the joint fight.

While this article is AF-centric, the cyber fight is joint and interagency, and as such, programs such as this should be open to all future leaders in cyberspace warfare.

B.10 How does this proposal fit into the Cyber Force Development Effort?

It is consistent with the Air Force mandate to develop operationally capable cyber warfare officers. The Air Force, under the guidance of Headquarters Air Force/A3 and Air Force Cyber Command (Provisional), has spent more than two years developing a strategy to organize and train the new cyber warfare forces.[65] The development effort culminated in April 2008 with an official Air Force strategy for developing cyberspace professionals. In it the SECAF and CSAF called for development of trained and educated warriors capable of tailoring cyber effects against enemy centers of gravity and integrating those seamlessly with the full-spectrum of Air Force and joint kinetic and non-kinetic effects.

B.11 What are the downsides?

The Air Force has too few officers in the field already. Having officers in school for an additional year represents a significant burden. There are also management and Permanent Change of Station (PCS) costs to consider, a significant issue in today's budget-constrained environment. These are real costs and cannot be downplayed; however, they represent an investment in the Air Force's cyber capability that will pay substantial dividends. Fortunately, due to recent decreases in student flows, AFIT has sufficient capacity to absorb 15-20 additional ICW students. Therefore, the majority of the programmatic costs will be management overhead and PCS expenses.

B.12 Potential Courses of Action (COA)

If the concept of a second year school to develop cyber-oriented warrior-scholars makes sense for the AF, there are at least three possible courses of action:

B.12.1 COA #1: Establish a new Air Force program consisting of ACSC and ICW.

This program would parallel the ACSC to SAASS program, and consist of the resident ACSC program at Maxwell AFB followed by the resident AFIT ICW program at Wright-Patterson AFB. Students would be competitively chosen from the 11X, 12X, 13S, 14N, and 33X AFSC in-residence school graduates, and placed in key positions after program completion.[66] Program timelines would match those of ACSC/SAASS.

Pros: The graduates from this program would have an in-depth understanding of the operational art of war and employment of airpower from ACSC, and an in-depth understanding of cyber warfare and how to create cyber power from AFIT's ICW. They would be both technically and operationally proficient, which would enable them to provide the innovative thought needed to develop cyber power as a warfighting function, as well as be respected and influential leaders of the cyberspace forces. Because their selection for in-residence school has already identified them as likely future senior leaders, they are more likely than average to be placed in key positions following the program. Finally, ACSC teaches officers how to use airpower to fight and win at the operational level of war. The cyber education from AFIT's ICW would enable the cyber power advocates to integrate both kinetic and non-kinetic capabilities across the warfighting spectrum.

Cons: The primary downside to this COA is cost. Officers in the program are out of the fight for two years, and it would involve two PCSs - one to ACSC and another to AFIT.

B.12.2 COA #2: Send more officers through AFIT's ICW.

Students would be selected from the 11X, 12X, 13S, 14N, and 33X IDE in-residence list, sent to AFIT along the lines of the current IDE program, and placed in key cyber and related positions after program completion.[67]

Pros: No significant programmatic or management changes need occur. This option also incurs only one IDE-related PCS and the students would only be out of the fight for one year.

Cons: The primary downside to this option is that the graduates would not have the in-depth education in operational art and the science of war provided by the in-residence ACSC program. The lectures and in-depth seminar discussions of the in-residence program add substantially to a student's understanding of the material. This discrepancy may decrease the graduates' ability to integrate cyber power with air and space power.[68]

B.12.3 COA #3: Combine AFIT's ICW and SAASS.

This program combines both AFIT's ICW program and SAASS. Students are competitively chosen from the 11X, 12X, 13S, 14N, and 33X AFSC in-residence school graduates. They are first sent to AFIT for ICW, and then sent to Maxwell for SAASS. Upon graduation from SAASS, they are placed in key cyber and related positions.[69] Program timelines match those of ACSC/SAASS.

Pros: The graduates from this program would have an in-depth technical and theoretical understanding of cyber warfare, and would be able to contribute that understanding effectively at SAASS. The non-cyber officers will gain an enhanced understanding of cyber. Having the airpower, space power, and cyber power strategists all in the same room will result in leaders able to think strategically across all three domains.

Cons: The primary downside to this COA is the same as COA #2—the lack of in-depth education in operational art and science. A second downside is the limited number of slots available in SAASS. Finally, this COA shares the cost downsides of COA #1. Officers in the program are out of the fight for two years, and would require two PCSs - one to AFIT and another to ACSC.

B.12.4 COA #4: Recreate the AFIT ICW program at Maxwell.

This program parallels the ACSC to SAASS program, and consists of the resident ACSC program followed by the Maxwell ICW program. Students are competitively chosen from the 11X, 12X, 13S, 14N, and 33X AFSC in-residence school graduates, and placed in key cyber and related positions after program completion. Program timelines match those of ACSC/SAASS.

Pros: The same as COA #1.

Cons: The primary downsides to this COA involve the difficulty and expense of duplicating technical engineering and science educational capability that exists at AFIT. The AFIT ICW program requires classified and unclassified laboratory and classroom space, classified and unclassified network connectivity, and extensive technical equipment. The most significant difficulty would be creating and maintaining an appropriate faculty. It takes many years to develop an effective, graduate level engineering faculty. Finally, one of the main advantages of AFIT's ICW curriculum is that the faculty members are part of the Air Force CyTCoE. This association allows them to stay on the leading edge of cyber warfare through teaching, research, and outreach—an advantage not available to faculty at Maxwell. The final downside is that officers in the program would be out of the fight for two years.

B.13 Cyber ACTS/SAASS Recommendation and Conclusion

I recommend COA #1: Establish a new Air Force program dedicated to developing cyber-oriented warrior-scholars. While expensive in terms of time and an additional PCS cost, it offers the best education to the officers in the program. This is cost-beneficial for the AF in terms of nurturing the most capable cyber warfare strategists. COA #2, increasing the number of students in the current AFIT ICW program, has the disadvantages discussed above, but may serve well as an initial step while the programmatics of COA #1 are being developed. COA #3, duplicating the ability to teach an ICW-like program at Maxwell is the least viable option, primarily due to the duplication of capabilities as well as the high cost.

This may not need to be a permanent program—the Air Force's abilities to fly, fight, and win in cyberspace will likely solidify into mainstream processes in ten to fifteen years. Until then we need to look back at how graduates of the Air Corp Tactical School and SAAS were able to make the most of the new capabilities airpower provided. Following this model will enable the Air Force to fully develop cyber power and enable its seamless integration into our warfighting capabilities. AFIT's ICW program is already up and running and can accommodate 15-20 additional students each year. I recommend the Air Force follow the ACTS/SAAS/SAASS path by creating a second year graduate path, emphasizing cyber, which parallels SAASS. Just as all second year PME graduates have been influential in developing American warfighting power to its current heights, the ICW graduates will be innovative, forward thinkers able to guide our Air Force towards a future in which we can counter all potential adversaries in all the domains in which we operate - air, space and cyberspace.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

[1] Wynn, Mosely, “SECAF/CSAF Letter to Airmen” and Mosely, “Operational Cyberspace Command ‘Go Do’.”
[2] Gates, "Secretary Gates Remarks at Maxwell-Gunter”.
[3] AF/A3O-CF, *Air Force Roadmap for the Development of Cyber Professionals.*
[4] JP 1-02, *Department of Defense Dictionary*, 141.
[5] Ibid.
[6] Ibid., 113.
[7] Ibid.
[8] Ibid.
[9] Ibid.
[10] Ibid., 263.
[11] JP 3-13, *Information Operations,* II-1.
[12] AFDD 2-5, *Information* Operations, 4.
[13] AFDD 2-11.
[14] Franz, *IO FOUNDATIONS TO CYBERSPACE OPERATIONS*, 51-52.
[15] Ibid., 66.
[16] Thomas, *Dragon Bytes,* 18-23.
[17] Landrieu, “Combating threats from cyberspace.”
[18] BBC, "Three million hit.”
[19] UPI, “Virus strikes 15 million.”
[20] Willsher, “French fighter planes grounded.”
[21] Traynor, “Russia accused of unleashing cyberwar.”
[22] Wentworth, "You’ve Got Malice.”
[23] AFIT, *IDE Cyber Warfare Program*.
[24] AFDD 1-1, *Leadership and Force Development*, 26.
[25] SAASS.
[26] Chiabotti, “A Deeper Shade of Blue.”
[27] US Army CGSC, “Command & General Staff,” and US Navy NOPC, “Joint Military Operations Naval,” and US Marine Corps SAW, “School of Advanced Warfighting.”
[28] Joint Advanced Warfighting School, ““Joint Advanced Warfighting School.”
[29] AFIT, *IDE Cyber Warfare Program*.
[30] The 33S (communications and information officer) and some 12X (navigator and electronic warfare officer) AFSCs are converting to 17D (for non-rated officers) and 12W (for rated officers) cyber warfare officers in 2009 or 2010. For the purpose of this essay, 33S and 12X are interchangeable with 17D and 12W.
[31] Other AFSCs such as the 61/62/63 family of scientists and engineers would undoubtedly benefit from this program as well. However, they are unlikely to lead cyber forces so the emphasis should be on those AFSCs most likely to capitalize on their cyber skills in the warfighting domains.
[32] Thomas, *Dragon Bytes,* 18-23.
[33] Landrieu, “Combating threats from cyberspace.”
[34] BBC, "Three million hit.”
[35] UPI, “Virus strikes 15 million.”
[36] Willsher, “French fighter planes grounded.”
[37] Traynor, “Russia accused of unleashing cyberwar.”
[38] Wentworth, "You’ve Got Malice.”
[39] Hansen, “Red Flag; A Realistic Training Environment,” 171-178.
[40] McBride, "Air Force Cyber Warfare Training."
[41] Ibid.
[42] Hansen, Andrew. *“*CYBER FLAG,” 76-96.
[43] US Army TRADOC, “Army approves plan.”

[44] Ibid.

[45] Ibid.

[46] JP 5-0, *Joint Operation Planning*.JP 5-0.

[47] AFIT, *IDE Cyber Warfare Program*.

[48] Thomas, *Dragon Bytes*, 18-23.

[49] Landrieu, "Combating threats from cyberspace."

[50] AFDD 1-1, *Leadership and Force Development*, 26.

[51] Hughes, *Over Lord*.

[52] Griffith, *MacArthur's Airman*.

[53] Van Creveld, *Command in War*.

[54] SAASS.

[55] Chiabotti, "A Deeper Shade of Blue."

[56] US Army CGSC, "Command & General Staff," and US Navy NOPC, "Joint Military Operations Naval," and US Marine Corps SAW, "School of Advanced Warfighting."

[57] Joint Advanced Warfighting School, ""Joint Advanced Warfighting School."

[58] SAASS.

[59] Gorman, Commandant, School for Advanced Air and Space Studies, personal interview with the author, 7 Jan 2009.

[60] Lt Col Bertrand Sparrow, DEI Deputy Chair, Air Command and Staff College, Maxwell AFB, AL, e-mail to the author, 14 Oct 2008.

[61] AFIT, *IDE Cyber Warfare Program*.

[62] AFIT, CCR.

[63] Husband, "The USAF's Need."

[64] The 33S (communications and information officer) and some 12X (navigator and electronic warfare officer) AFSCs are converting to 17D (for non-rated officers) and 12W (for rated officers) cyber warfare officers in 2009 or 2010. For the purpose of this essay, 33S and 12X are interchangeable with 17D and 12W.

[65] For an early description of that effort, see Franz, "Defining Information Operations Forces," 53–63.

[66] Other AFSCs such as the 61/62/63 family of scientists and engineers would undoubtedly benefit from this program as well. However, they are unlikely to lead cyber forces so the emphasis should be on those AFSCs most likely to capitalize on their cyber skills in the warfighting domains.

[67] Ibid.

[68] At the time of this writing, the author is nearing the end of the in-residence ACSC program. He completed the non-resident program in 2007.

[69] Other AFSCs such as the 61/62/63 family of scientists and engineers would undoubtedly benefit from this program as well. However, they are unlikely to lead cyber forces so the emphasis should be on those AFSCs most likely to capitalize on their cyber skills in the warfighting domains.

Bibliography

AF/A3O-CF. *The Air Force Roadmap for the Development of Cyberspace Professionals 2008-2013 (U\\FOUO)*. Washington, DC, 2008. Information referenced is not FOUO.

Air Force Doctrine Document (AFDD) 1-1, *Leadership and Force Development*, 18 February 2006.

AFDD 2-5. *Information Operations*, 11 January 2005.

AFDD 2-11 (Draft). *Cyberspace Operations*, 31 November 2008.

Air Force Institute of Technology (AFIT). Center for Cyberspace Research (CCR). http://www.afit.edu/ccr/ (accessed 7 Oct 2008).

Air Force Institute of Technology (AFIT). *IDE Cyber Warfare Program Guide.* http://www.afit.edu/en/eng/PDF/Program%20Guide%20-%20Cyber%20Warfare2.pdf (accessed 3 Oct 2008).

Air Force School of Advanced Air and Space Studies (SAASS). "SAASS Home". http://www.au.af.mil/au/saass/ (accessed 5 April 2009).

BBC. "Three million hit by Windows worm". BBC News Online (BBC). 16 January 2009. http://news.bbc.co.uk/1/hi/technology/7832652.stm (accessed 3 April 2009).

Chiabotti, Stephen D. "A Deeper Shade of Blue: The School of Advanced Air and Space Studies." *Joint Force Quarterly*. National Defense University Press, issue 49, 2nd quarter, 2008.

Franz, Timothy P. *IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way-Ahead for Network Warfare Forces*. Wright-Patterson Air Force Base, OH: Air Force Institute of Technology, Department of Electrical and Computer Engineering, 2007.

Franz, Timothy P. and Durkin, Matthew F. and Williams, Paul D. and Raines, Richard A. and Mills, Robert F. "Defining Information Operations Forces: What Do We Need?" *Air and Space Power Journal* 21, no. 2 (Summer 2007).

Gates, Robert. "Secretary Gates Remarks at Maxwell-Gunter Air Force Base, Montgomery Alabama" (transcript). 21 April 2008. DefenseLink News (U.S. Department of Defense). http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=4214 (accessed December 23, 2008).

Griffith, Thomas, E. Jr. *MacArthur's Airman*. Lawrence, KS: University of Kansas Press, 1998.

Hansen, Andrew. *CYBER FLAG: A REALISTIC CYBERSPACE TRAINING CONSTRUCT*. Master's Thesis, Air Force Institute of Technology, 2007.

Hansen, Andrew, and Williams, Paul, and Mills, Robert. “Red Flag; A Realistic Training Environment for the Future”. *Proceedings of the 3rd International Conference on i-Warfare & Security*. University of Nebraska, Omaha, NE, 2008.

Hughes, Thomas Alexander. *Over Lord*. New York, NY: The Free Press, 1995.Hughes, Overlord.

Husband, D. Mark. “The USAF’s Need for More ‘Warrior-Scholar’ Senior Officers, Applying the Five Whys”. *The Wright Stuff,* Volume 3, Issue 3, 14 February 2008. http://www.maxwell.af.mil/au/aunews/archive/0303/Articles/TheUSAFsNeedforMoreWarriorScholarSeniorOfficers.html (accessed 10 Oct 2008).

Joint Advanced Warfighting School, “Joint Advanced Warfighting School (JAWS)”. http://www.jfsc.ndu.edu/schools_programs/jaws/overview.asp (accessed 6 Jan 2009).

Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms,* 12 Apr 2001 (as Amended through 17 Oct 2008).

JP 3-13. *Information Operations,* 13 February 2006.

JP 5-0. *Joint Operation Planning*, 26 December 2006.

Landrieu, Mary. “Combating threats from cyberspace.” The Hill, 17 Jun 2008. http://thehill.com/op-eds/combating-threats-from-cyberspace-2008-06-17.html (accessed 15 Nov 2008).

McBride, Aaron. "Air Force Cyber Warfare Training". *Defense Standardization Program Journal*. Defense Standardization Program Office, Fort Belvoir, VA, Apr 2007.

Moseley, Michael W. Wynn and T. Michael. "SECAF/CSAF Letter to Airmen: Mission Statement." edited by USAF, 2005.

Thomas, Timothy L. *Dragon Bytes, Chinese Information War Theory and Practice*. Fort Leavenworth, KS, Foreign Military Studies Office, 2004.

Traynor, Ian. “Russia accused of unleashing cyberwar to disable Estonia.” The Guardian, 17 May 2007. http: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (accessed 3 April 2009).

UPI. “Virus strikes 15 million PCs.” UPI.com, January 26 2009. http://upi.com/Top_News/2009/01/25/Virus_strikes_15_million_PCs/UPI-19421232924206 (accessed 3 Apr 2009).

US Army Command and General Staff College (CGSC). “Command & General Staff”. http://usacac.army.mil/CAC2/cgsc/ (accessed 6 January 2009).

US Army Training and Doctrine Command (TRADOC). "Army approves plan to create school for Red Teaming". http://www.tradoc.army.mil/pao/tnsarchives/july05/070205.htm, (accessed 3 Dec 2008).

US Navy Naval Operational Planner Course (NOPC). "Joint Military Operations Naval Operational Planner Course (NOPC)". http://www.nwc.navy.mil/academics/courses/jmo/nop.aspx (accessed 6 January 2009).

US Marine Corp School of Advanced Warfighting (SAW). "School of Advanced Warfighting". http://www.tecom.usmc.mil/mcu/csc/saw/index.htm (accessed 6 Jan 2009).

Van Creveld, Martin. *Command in War*. Cambridge, MA: Harvard University Press, 1985.

Wentworth, Travis. "You've Got Malice: Russian nationalists waged a cyber war against Georgia. Fighting back is virtually impossible." Newsweek, 12 August 2008. http://www.newsweek.com/id/154965 (accessed 3 Apr 2009).

Willsher, Kim. "French fighter planes grounded by computer virus." The Telegraph, 7 February 2009. http://telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html (accessed 3 April 2009).

Wynne, Michael. "Letter to Airmen: Cyberspace Operations." 7 May 2007.